DE GRUYTER OPEN

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **17**, No 4
Sofia • 2017 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2017-0046

A Survey on Key(s) and Keyless Image Encryption Techniques

Ranjan Kumar H. S.[1], *Fathimath Safeeriya S. P.*[1], *Ganesh Aithal*[2], *Surendra Shetty*[1]

[1]*NMAMIT, Nitte, Udupi, Karnataka, India*
[2]*MITE, Moodbidri, Mangalore, Karnataka, India*
Email: ranjan@nitte.edu.in safeeriya@gmail.com ganeshaithal@gmail.com hsshetty@nitte.edu.in

***Abstract*:** *As in recent years digital data transmission and image application have been increasing, maintaining secure transmission of image is of high importance. Image Encryption is implemented to achieve security on image applications. This paper exhibits a survey on various existing image encryption techniques. The paper mainly focuses on two types: Image encryption with Key*(*s*) *and Image Encryption without Key*(*s*). *In addition it also describes several properties of a good image encryption technique. The paper presents a survey of most popular algorithms and research papers that are related with different image encryption techniques.*

***Keywords*:** *Chaotic sequence, image scrambling, error diffusion, visual cryptography, random grid.*

1. Introduction

With an impeditive growth in multimedia applications and network technologies, secure transmission of multimedia files must be guaranteed over untrusted networks. Various confidential data such as military communication, bank data, government identifications, personal image files are exchanged over internet. Hence, data must be authenticated and authorized with suitable encryption techniques.

While transmitting secret images, high security must be provided due to threats like hacking, spoofing, eavesdrops. These attackers utilize weak link over communication network to steal the information. Traditionally an appropriate image compression technique is applied on image data and its output is encrypted. This process can be reversed while decrypting. The process of image Encryption transforms an image such that it is difficult to understand or predict the original image. Image Encryption process includes application of best suitable algorithm and/or key(s) to convert original digital image into cipher image before they are transmitted or stored. Decryption involves application of same algorithm and same and/or different key(s) to get back the original data from cipher code.

This survey on Image Encryption is organised as shown in Fig. 1, Section 2 elaborates image encryption methods using key(s) and gives detailed description on most popularly used key(s) based algorithms along with a brief overview on few implemented techniques using those algorithms. Section 3 contains a detailed view on Visual Cryptography (VC) along with a brief overview on few related techniques using VC Schemes. This paper also extends the properties of a good key(s) and keyless image encryption separately.

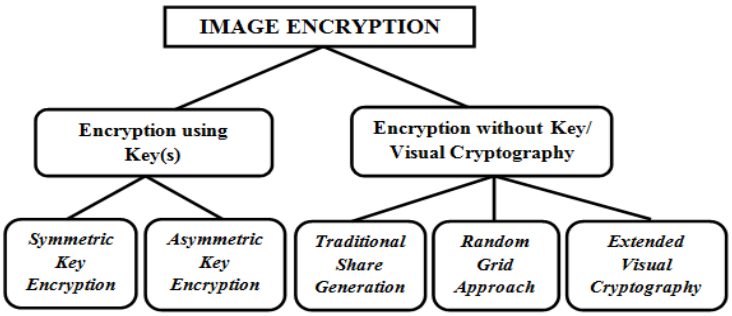


Fig. 1. Block-diagram of Image Encryption techniques

2. Image encryption using key(s)

Image Encryption using key is one of the effective ways of securing an image data by transforming or changing the input data using key(s) into a format that are unrecognizable. Image Encryption Process using key is shown in Fig. 2. A good encryption algorithm uses a strong key (the key that is almost impossible to be cracked by any intruder) to convert the plaintext image into encrypted image and the vice versa (i.e. decryption). The data is seen as random string of bits in encrypted format when an attacker intercepts it, hence the technique is secure. Key Management and Distribution is difficult and challenging task.

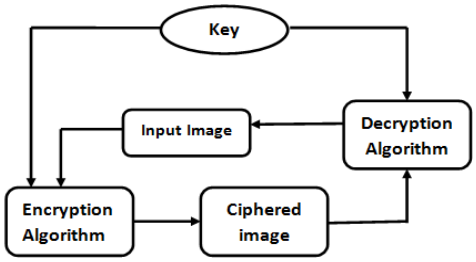


Fig. 2. Image encryption and decryption with key

2.1. Symmetric key cryptography

Symmetric key cryptography also called as *secret key encryption*. This approach uses same key for encryption as well as decryption. The execution uses two processes, Generation of Key than do encryption and Decrypt using the generated key. Major issue related to this approach is key distribution. Key distribution is done with the

transmission of the data and security of the data mainly depends on nature of the image, key generation algorithm and key size. In the next section few popular symmetric encryption algorithms are summarized along with few recent image encryption research works using the same.

- ***Data Encryption Standard* (*DES*) *algorithm*** is based on symmetric key block cipher developed earlier by IBM for Lloyd's of London for cash transfer. It is then adopted and published by National Institute of Standard and Technology in 1977. DES operates on block size of 64 bits a time, length of the key used is 64 bits (56 bits key and 8 bits are parity check bits) [1]. Initially input is split into 64 bits blocks. If input bits are unevenly divided with 64 then the last block is padded. Same key is used for both encryption and decryption. The encryption process holds two permutations (initial permutation and final permutation) and 16 rounds. The 64 bits block is subjected to initial permutation and then the block is split into two halves (right half and left half) each 32 bits long. Then there are 16 rounds of identical operations in which data is combined with the key in 4 steps in each 16 rounds:

Step 1. In each round, bits of the key are shifted and 48 bits are selected from 56 bits key length.

Step 2. Expand right half of 32 bits block to 48 bits using an expansion permutation.

Step 3. The 48 bits of shifted and permuted key is combined with 48 bits of block obtained in step 2 by XOR operation.

Step 4. The combination is sent through 8 S-boxes (Substitution boxes) to produce 32 bits and permuted again.

The output of these 4 steps is then combined with left half with XOR operation and the combined result is considered as new right half and old right half becomes new left half. After the completion of 16 rounds the right and left halves are combined and final permutation is done. The decryption process is same as that of encryption algorithm which takes cipher text as input but use key K_i in reverse order (i. e., K_{16} in first iteration, ..., K_1 in 16-th iteration).

Analysis shows that the DES algorithm exhibits a strong Avalanche effect [1]. DES is not resistant to Brute Force Attack since DES has only 2^{55} possible combinations. DES can be cracked using 2^{55} encryptions. Therefore this algorithm is less secure [2].

- *New image encryption scheme based on DES Algorithm and Chua's Circuit*: Qian Gong-Bin, Jiang Qing-Feng and Qiu Shui-Sheng [3] introduced a new method of image encryption using DES algorithm combined with chaotic systems. This paper illustrates the weaknesses of existing DES algorithm, i.e., small key space and iterating operations. The proposed method uses chaotic sequences generated by Chua's circuit as initial key. Chua's circuit is an electronic circuit which produces oscillator waveform which is non repetitive unlike ordinary oscillator. The circuit is a three dimensional self-oscillating with four linear elements: inductance L, resistance R, capacitor C_1, C_2 and non-linear resistance N_r which is called Chua's Diode. This method improves the initial key and iterative operation of DES algorithm. The author claims 'trap door' may exist due to non-availability of principle of *s*-box design. The recurrence and regularity of 16 round structures can be

eliminated by XOR-ing chaotic sequences sub key and right part of plaintext. The need of this mechanism is to make right part of plaintext no longer depend on sub key. Analysis shows that this method is capable of resisting attacks, expands the key space, and provides improved security for an input image.

○ *Image encryption algorithm based on chaotic map and S-DES*: Ling Bin, Liu Lichen and Zhang Jan [4] proposed a dual encryption algorithm using S-DES and Lu Map. The scheme is based on classical Arnold cat map Algorithm and S-DES. S-DES is a Simplified-DES which use of 8 bits blocks and pixels are consistent in a block. The key numbers of S-DES are increased and key can be changed in real time by using Lu chaotic. Lu chaotic map is a three dimensional chaotic map, which generates system trace (x, y, z) when system parameters a, b, c are fed into equation $x = a(y - x)$, $y = -xz+cy$, $z = xy - bz$. These values x_0, y_0, z_0 are used as systems initial value in $N \times N$ iterations to produce three sequences which are used in image encryption. Arnold cat map is a function that randomizes the positions of pixels inside an image and this function is applied to shuffle image using encryption process. The results show that the method is faster and well secured. The advantage of this method is easy to understand, operates in rapid encryption speed, and has large keys and sensitivity to initial value when compared to traditional method.

- ***Advanced Encryption Standard* (*AES*)** is a symmetric key encryption algorithm introduced by Joan Daemen and Vincent Rijmen (see [1]) to replace DES Algorithm. In 1988, the US National Institute of Standards and Technology (NIST) recommended the use of AES instead of DES. AES operates on block sizes of 128, 168, 192, 224, and 256 bits; key length of 128, 192, and 256 bits [5]. The standard encryption uses AES-128 where both the block and key size are 128 bits. The size of block and key decides the number of rounds in the process. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds [6]. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Each processing round involves four steps:

Step 1. Substitute bytes: Uses an S-box to perform a byte by byte substitution of the block.

Step 2. Shift rows – A simple permutation.

Step 3. Mix column – A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix.

Step 4. Add round key – The key for the processing round is XOR-ed with the data.

○ *A Composite image encryption scheme using AES and chaotic series:* Xiao Huijuan, Qiu Shuisheng and Deng Chengliang [7] proposed an image encryption scheme based on AES algorithm and chaotic series. Chaotic series is generated by logistic equation, where the parameters are modulated by another logistic equation with unique initial values. This algorithm uses chaotic series as a key to facilitate AES operations in temporal domain. The combination of chaotic and conventional encryption may result in very strong cryptosystems. In general, two

ways of these combinations are illustrated. The first one involves application of chaos encryption to the output of conventional encryption. The second combination is application of chaotic encryption to modify the conventional encryption algorithms. The image encryption involves two stages: 1) pixel values are modified using chaotic AES substitution; 2) pixel positions are permuted with the help of chaotic matrix. The algorithm promises integrity and confidentiality of a secret image.

- *Image encryption with the AES Algorithm in wireless sensor network:* Msolli, Helali and Maaref [8] proposed a scheme with modified AES algorithm to improve security in multimedia files of wireless sensor networks. The author claims that the design of AES algorithm is best suitable for wireless sensor networks. The main objective of any wireless sensor network is to reduce the energy consumption. According to author's research, reduction in the number of rounds in AES process also reduces the energy consumption. This algorithm uses simple computations, that is compatible with the nature of sensor nodes and increases the lifespan of sensor nodes. Analysis is done to check the performance of the algorithm. This algorithm allows encrypting the image in real time reducing execution time.

- ***Blowfish algorithm*** is introduced by Schneier [9] in 1993 which is designed for fast Encryption 32 bit microprocessors. Blowfish is symmetric key block cipher algorithm which replaces DES algorithm. The size of the block used in 64 bits and key can be from 32 bits to 448 bits in length. The algorithm works in two parts: Key expansion and data encryption. Data encryption process consists of 16 round structures, each round performs simple transformation. Each round performs key dependent permutation and key and data dependent substitution. 64 bits block is divided into two halves each 32 bits long. Encryption consists of two sub key arrays: 4 S-boxes (substitution boxes) and 18 P-array (permutation array) [10]. All encryption operations are XOR and addition of 32 bit blocks in 16 iterations. The output obtained 64 bits cipher text which is obtained by concatenation of two halves produced after the round operation. The key expansion process includes XOR operation on P_1 array and the 32 bits key, P_2 array is XOR-ed with next 32 bits of key, until P_n array. These sub keys are used in data encryption process. No attacks cracked the algorithm yet. This is highly secure and fastest algorithm though it suffers from weak key issues.

- ***Image encryption using Block-Based Transformation Algorithm.*** Ali, Younes and Jantan [11] proposed a new block-base image transformation algorithm. The algorithm is based on combination of image transformation and blowfish algorithm. The secret key which is used to determine the seed value is fed to transformation algorithm to generate transformation table. The values of the transformation table are used as new location to transform an image block. Image transformation is carried out by splitting the original image into random blocks which holds specific number of pixels and these blocks are scrambled within the image using new location fetched from transformation table. The transformed image is then subjected to blowfish algorithm to obtain encrypted image. In this proposed method the correlation between image elements is decreased, hence it is hard to predict the value of any pixel from the value of its neighbours. The entropy is increased as the

number of blocks increases. This technique has better performance when compared to other algorithms by measuring its entropy and correlation.

- ***RC4*** is one of the most popular algorithms proposed by Ron Rivest (see [12]). The main design principle of RC4 is to extract pseudorandom bytes from pseudorandom permutations. The process consists of two components: the Key Scheduling Algorithm (KSA) and the PseudoRandom Generation Algorithm (PRGA). The KSA performs the initial pseudorandom permutation of algorithm by scrambling an identity permutation with the use of secret key *k*. The output of the initial permutation performed by the KSA is used as an input to the PRGA that generates the key stream. RC4 key can be used only once and it is 10 times faster than that of DES algorithm. This algorithm is vulnerable to attacks and suffers from weak keys [14]. The steps for RC4 encryption algorithm [13] are five.

Step 1. Input the data to be encrypted and the selected key.

Step 2. Initialise two string arrays: assign array 1 with numbers ranging 0-255 and array 2 with the selected key.

Step 3. Randomize array 1 depending on the array 2.

Step 4. Randomize array 1 within itself to generate the final key stream.

Step 5. XOR the final key stream with the plaintext to give cipher text.

○ *Digital colour image encryption using RC4 stream cipher and chaotic logistic map:* Riah Ukur Ginting and Rocky Yefrenes Dillak [15] proposed a new stream cipher algorithm based on RC4 and chaotic logistics map. The proposed scheme has following steps:

Step 1. Set initial value x_0 by converting the external key of 16 ASCII characters each of 8 bits.

Step 2. Generate a key stream array with initial value using Chaotic Logistic Map (CLM) function. CLM uses a simple non-linear dynamical equation which is very sensitive to initial values. The general form of CLM is $X_{n+1} = \lambda X_n(1 - X_n)$ where λ is the control parameter on $0 \leq \lambda \leq 4$ and X_n is real number.

Step 3. Permutation unit: In initial permutation, the key stream array that is obtained from Step 2 is swapped with array *S* which consist values from 0 up to 255 in ascending order. In final Permutation, the result of initial permutation is XOR-ed with digital image. Since external key is very sensitive, any changes in the key the output will be totally different.

○ *Fast partial image encryption scheme with wavelet transform and RC4:* Sapna and Deepu [16] proposed a new scheme which uses Discrete Wavelet Transform (DWT) and RC4 Algorithm. DWT is a mathematical function that transfers the original signal from time domain into time-frequency domain. Daubechies wavelets are used in this algorithm; they are specific occurrence of conjugate quadrature filters. In this method only a part of the image is encrypted and rest is shuffled using proposed shuffling algorithm. Initially RC4 Algorithm is used to generate the key stream. The original image is subjected to DWT and produces four coefficient matrices: approximation (C_a), horizontal (C_h), vertical (C_v) and diagonal (C_d) matrices. The lowest frequency sub band matrix C_a, will hold most of

the image information, thus matrix C_a is used in encryption. The matrix C_a is encrypted by XOR-ing the generated key stream and matrix C_a. Since a part of image is encrypted it is easy for the intruder to gain information from other three coefficients. Therefore C_h, C_v, C_d matrices will be shuffled, which increases the level of security. Proposed Shuffling algorithm works in two stages: First stage, a new location value is obtained for each block by performing modulus operation between key and size of the matrix (row×column). Second stage, swap each image block with the new value to obtain shuffled image. Finally, encrypted image obtained by inverse discrete wavelet transform of encrypted matrix and shuffled matrices. Much time is saved by encrypting only a part of the image. The system only encrypts the lowest frequency band of the image.

- ***International Data Encryption Algorithm* (*IDEA*)** is proposed by Xuejia Lai and James Massey in 1990 (see [1]). This algorithm is an extension of initial proposal of the *Cipher Based Differential Cryptanalysis by Biham and Shamir*. IDEA operates on 64 bits of data block and a key of 128 bits long. The aim behind IDEA design is "mixing of arithmetical operations from different algebraic groups" [1]. The algorithm works with two processes: Round transformation and Key scheduling. In Round Transformation the 64 bits data is further divided into four blocks each 16 bits long. Each of the four blocks is processed through eight rounds and transformed by XOR operations: Addition modulo 2^{16} and multiplication modulo $2^{10}+1$. The cipher obtained is much needed non linearity from these operations and does not require an explicit S-box for the process. Key Scheduling process, the 128 bits long key is further split into eight blocks of 16 bits length. During encryption each key blocks are used during iterative rounds of round transformation. Decryption is same as that of encryption, but the key blocks are used in reverse order.

  - *New efficient image encryption technique based on Arnold Algorithm and IDEA Algorithm:* Riad et al. [17] proposed a new image Encryption technique based on IDEA and chaotic Arnold's Cat Map (ACM). Initially, IDEA generates encryption key using 128 bits secret key. This encryption key is used to generate the encryption matrix where it requires successive rotations from encryption key to form rows of the encryption matrix. Primary encrypted image is produced by XOR-ing the input image and encryption matrix. Finally, fully encrypted image is formed by shuffling positions of primary encrypted image pixels using ACM. ACM transformation involves shearing a square image. Shearing of an image is done on x axis (horizontal shear) and y axis (vertical shear), in which horizontal shear takes point with coordinate (x, y) to the new point $(x+my, y)$ and vertical shear takes point with coordinate (x, y) to the new point $(x, y+mx)$, where m is shear factor. In ACM shear factor is always equal to 1. It stretches the image of $n \times n$ pixels and wraps the stretched portion to regain the original dimension of the image. Analysis shows that proposed scheme is efficient, highly key sensitive and secure. Since encryption matrix is generated using key blocks to obtain encrypted image, the run time of new method is much smaller than that of IDEA.

  - *Secure-International Data Encryption Algorithm* (*S-IDEA*): Singh, Verma and Mishr [18] proposed a secure encryption algorithm based on IDEA. The proposed method has two features: increased size of key and increased degree of

diffusion thus strengthens existing IDEA by overcoming large weak key problem and newly detected attack on round 6 of IDEA. In this method, size of the key is increased to 256 bits from 128 bits which increases the complexity of the algorithm for secure encryption. There are eight encryption rounds in the process. In first round two key sub-blocks (16 bits) are combined. Two Multiplicative Additive (MA) blocks are used in a single round of IDEA to increase the amount of diffusion. These MA blocks are used. With this extension of original IDEA, the proposed method provides good cryptographic strength.

- ***Hill Cipher*** is a polygraphic substitution cipher based on linear algebra which is proposed by Lester S Hill in 1929 (see [19]). Hill Cipher algorithm is a symmetric key encryption algorithm. The core of this algorithm is matrix manipulation. To encrypt a message, select an $n \times n$ matrix E which must be an invertible modulo of 26.This serves as encryption key. Convert each letter of the plaintext to number between 0 and 25. Split the string of numbers into block size n and write each block as column vector of size n. The message is a sequence odd n dimensional vector, $v_1,..., v_t$. Multiply each vector with matrix E. Place the entries of vectors in order and convert the number back to characters to obtain cipher text. To decrypt a cipher text, compute $D = E^{-1} \pmod{26}$ where D is the decryption key. Convert the cipher text into matrix C. Compute $DC = M$, where M is the matrix holding plaintext messages. The hill cipher is not be used on its own, since it is not secure. This algorithm is a useful step when combined with other non-linear operations, such as S-boxes (in modern ciphers).

  ○ *Image encryption using advanced Hill Cipher Algorithm:* Bibhudendra et al. [20] proposed a novel encryption method based on Hill Cipher Algorithm which uses an involuntary key matrix and this method overcomes problems of encrypting image with homogenous background. The advanced Hill Cipher Algorithm includes four steps:

  Step 1. An involuntary key matrix ($m \times m$) is generated by selecting any arbitrary ($n/2 \times n/2$).

  Step 2. Divide the original image in symmetric blocks of size $m \times m$.

  Step 3. Hill cipher is applied on temporary blocks which are formed by bringing together i-th pixel of each block. Hill cipher is again applied to transposed resultant matrix.

  Step 4. The matrix obtained will be added to the i-th block of encrypted image to generate final encrypted image. In this technique, process of finding inverse of matrix for decryption is completely eliminated and use of involuntary key matrix during encryption reduces computational complexity. Comparison of proposed scheme with existing method shows that proposed scheme is faster, secure and robust.

  ○ *Grayscale-image encryption using random Hill Cipher over $SL_n(F)$ associated with discrete wavelet transformation:* Mishra and Sharma [21] proposed a novel method for gray scale image encryption and decryption based on Random Hill Cipher (RHC) over $SL_n(F)$ associated with Discrete Wavelet Transformation (DWT). $SL_n(F)$ is general linear group of $n \times n$ matrices with

determinant 1 which forms a group under multiplication over F. In RHC the hill cipher keys will be chosen from special linear group with degree and Field F (i.e., $SL_n(F)$) for image matrix. The input image is divided into equal blocks ($m \times m$), in which size of sub-block will be same as that of hill cipher key chosen from $SL_n(F)$ domain such that n divides m. Two Stage Random Hill Cipher (TSRHC) is used. In the first stage RHC is applied before DWT and the second stage involves applying RHC after DWT. DWT decomposes the original image in four sub images, the sub image with lowest frequency sub image is encrypted. In encryption process, initially first stage RHC is applied to generate partially encrypted image and then subjected to DWT. Two dimensional DWT is carried out for rows and columns separately. The second stage RHC is applied to the output of DWT to generate fully encrypted image. Decryption is the inverse of encryption process. This method uses matrix multiplication in hill cipher which is non commutative. So decryption relies on pre or post multiplication of inverse hill cipher keys with encrypted gray scale image on the same location of hill cipher keys used in encryption process. Thus this method provide strong security, the attacker cannot decrypt image without knowing information about location.

- ***Chinese Remainder Theorem* (*CRT*).** Let $p_1, p_2, ..., p_n$ be a collection of pair wise relatively prime numbers, then the system of simultaneous congruences $X \equiv r_1 (\text{mod } m_1)$, $X \equiv r_2 (\text{mod } m_2)$, ..., $X \equiv r_n (\text{mod } m_n)$ has a unique solution modulo $M = m_1, m_2, ..., m_n$ and $r_1, r_2, ..., r_n$ are given integers (residues). The CRT enables the conversion of residues back into more traditional form such as Decimal form. With this theorem, for residues $\{r_1, r_2, ..., r_n\}$ of a number X, can be converted back into X, provided the greatest common divisor of any pair of modulo is 1. The theorem can be expressed as

$$X = \sum_{i=1}^{N} A_i T_i r_i \left(\text{mod } M\right), \tag{1}$$

where, r_i is the residue, A_i is M/m_i, M is the product of modulo, and T_i is the multiplicative inverse of m_i.

○ *Image encryption algorithm based on chaotic mapping and Chinese remainder theorem:* Yang, Hua and Jia [22] proposed an image Encryption method based on CRT and chaotic mapping. Chebyshev mapping is a chaotic mapping of one dimensional sequence. The expression for k order Chebyshev mapping is: $x_{n+1} = \cos(k \times \arccos(x_n))$, where the value of x_n is between –1 and 1 and the system enters chaotic state when $k \geq 2$. The main aim of the proposal is to improve the security of the encryption algorithm. There are two features used: pixel scrambling and image diffusion. Initially a chaotic sequence is generated using Chebyshev mapping and this sequence is used to scramble the image pixel. Finally, scrambled image is changed by applying CRT (as described in previous section) and Fibonacci series. This method can resist correlation attack.

2.1.1. Recently proposed symmetric image encryption methods

○ *New image encryption algorithm based on chaos:* Kong and Li [23] presented a new technique based on Chen's chaotic system, cellular automation and DNA. Chen's chaotic system is a three dimensional system, generates pseudo random

numbers can be stated as: $x= a(y – x)$; $y=(c – a)\ x – xz + cy$; $z = xy – bz$ where a, b and c are control parameters. A cellular automation is non-linear dynamic system, each element is equal to its cell and each cell has finite state. The proposed technique uses one dimensional cellular automation with two neighbours that is left and right neighbours and consists of two states 0 and 1. Biologically, DNA sequence consists of four bases and complementary base pairing rule exist between the four bases. This principle is used in image encryption process, a grey scale image is represented by 8 digit binary number and every two digit is represented by four bases. Initially, a pseudo random number is generated by 3-dimensional Chen chaotic systems to complete dynamic DNA encryption of plain image and then based on the sequence transformed, cipher image is produced. The pixels of the encrypted cipher determine the evolution of the cellular automation. Finally, DNA sequence of the image is split into blocks and then combines these blocks with DNA sequence of cellular automation. The mixed operation is carried out with cipher text diffusion mechanism to get the final DNA and it is decrypted. The analysis result shows that the proposal is efficient and resists attack.

○ *Image encryption and compression based on Kronecker compressed sensing and elementary cellular automata scrambling:* Chen Tinghuan et al. [24] presented an image scrambling technique based on encryption and compression with combination of Kronecker Compression Sensing (KCS) and Elementary Cellular Automata (ECA). Difference of sparsity levels among blocks of the sparsely transformed image is the motivation behind this technique. There are two stages for encryption: In initial stage, sparsity levels are uniformized by scrambling sparsely transformed image using ECA. ECA is the simplest operation of one dimensional cellular automaton with two possible values (0 or 1) for each cell and depends only on nearest neighbour values. In the second stage, to sort out low complexity and storage issues the scrambled and sparsely transformed image is encrypted and compressed using KCS. KCS is the method used to reconstruct all the vector reshaped blocks of a multi-dimensional signal to a vector and it is also used to permute measurement matrices for compressed sampling blocks to diagonal structured matrix. This technique has great performance in terms of scrambling and uniformity of sparsity levels and the encryption-compression method provides better secrecy and flexibility.

○ *Image encryption using 2D logistic-adjusted-sine map*: Hua and Zhou [25] introduced a new chaotic map which has wider chaotic range than many existing chaotic maps and presented a new image encryption scheme based on newly proposed chaotic map. Initially it proposes a new chaotic map called Two Dimensional Logistic-Adjusted-Sine Map (2D-LASM). Logistic map is a polynomial mapping in which chaotic behaviour can be derived from a non-linear dynamic equation: $x_{i+1} = 4px_i(1 - x_i)$, where p is a parameter on $0.89 \leq p \leq 1$. Sine map is similar to logistic map, it is sine function by transforming the input into the closed unit interval derived as $x_{i+1} = s\sin(\pi x_i)$, where s is a parameter on $0.89 \leq s \leq 1$. 2D-LASM uses logistic map to adjust input of sine map and then extends its phase plane from 1D to 2D. 2D-LASM is derived using sine map and logistic map with mathematical equation as in (2), where $0 \leq \mu \leq 1$ which is computed using sine map and logistic map:

$$\begin{cases} X_{i+1} = \sin(\pi\mu(y_i + 3)x_i(1 - x_i)), \\ Y_{i+1} = \sin(\pi\mu(x_i + 1 + 3)y_i(1 - y_i)). \end{cases} \quad (2)$$

2D-LASM has more complex structure and result is difficult to predict when compared with sine map and logistic map. In addition, the paper introduced a 2D-LASM based Image Encryption Scheme (LAS-IES) using 2D-LASM. The scheme contains mainly three components: 1) adding surrounding pixels; 2) bit manipulation confusion; 3) bit manipulation diffusion. Adding surrounding pixels – security of the encrypted image is improved by mechanism of adding random values to the input image. Bit manipulation confusion and bit manipulation diffusion – the scheme performs multiple rounds of confusion and diffusion operation at bit level. The scheme is capable of resisting various kinds of attacks.

o *Multiple-image encryption with bit-plane decomposition and chaotic maps:* Zhenjun Tang et al. [26] introduced an image encryption algorithm which can work with multiple grey scale images. Initially the algorithm decomposes input of four grey scale images into bit planes(each pixel will be represented into 8 bit binary sequence and then grey scale image is decomposed into 8 bit planes). Henon map is applied to determine the random bit block pattern. Henon map is a two dimensional map that takes point (x_n, y_n) on a plane and maps it to a new point. It is defined as

$$\begin{cases} x(k+1) = 1 - ax_2(k) + y(k), \\ y(k+1) = bx(k), \end{cases} \quad (3)$$

where a and b are control parameters, initial values $x(0)$ and $y(0)$ are taken as secret keys.

Two chaotic sequences are generated from this equation. The arrays of storing block size D and overlapping sizes F are obtained by $D[k]$ = mod(mod($x(k)\times 2^{48}$, 256), 69) + 32 and $F[k]$ = mod($y[k]\times 2^{48}$, $D[k]$ − 1) + 1. Bit planes are randomly split into overlapping bit blocks and bit blocks are swapped with different bit planes randomly. Finally, four chaotic images are generated by applying XOR between four shuffled image and secret matrix which are controlled by logistic map. Encrypted PNG is generated by viewing four chaotic images as alpha, red, green and blue as its components. Security of the proposed algorithm is improved by using several secret keys. This algorithm is applicable to batch processing of large scale image database with high performance.

o *Image scrambling encryption algorithm of pixel bit based on chaos map:* Ye [27] introduced this algorithm. Initially, a grey scale image is read and pixel values are assigned to a matrix ($M\times N$). The algorithm implements grey scrambling of an image using single chaos map where values of the pixel ranging from 0-255 are distributed evenly and then pixel positions are permutated. Matrix A is decomposed into bit pixels assigned to matrix B ($M\times 8N$). The row and columns of matrix B is encrypted based on logistic map to obtain matrix C. Matrix C is then converted to matrix with decimal values, that is matrix D by formula as

$$P(i, j) = \sum_{t=0}^{7} 2^t p^t(i, j), \quad (4)$$

where $P(i, j)$ is the pixel position in matrix A and $p^t(i, j)$ is transformed pixel position values. The original image is completely transformed and encryption

is complete; it increases the difficulty of an unauthorized one to crack the encrypted data. This algorithm serves large key space, key sensitivity and high scrambling degree. This is applicable for providing security of digital image data over the internet.

○ *Image encryption based on independent component analysis and Arnold's cat map:* Nidaa and Abbas [28] presented a new efficient image encryption technique based on chaotic Arnold's Cat Map (ACM). This algorithm modifies the mixing matrix in Independent Component Analysis (ICA). ICA is a model in which the data variables are considered to be linear or non-linear mixture of some unknown latent variable and mixing system. Initially, ACM is used to generate a mixing matrix by inputting a square image of any dimensions. In the second stage, implementation of mixing process is carried out by mixing matrix and image sources to generate encrypted images that depend on the number of sources. Finally, this encrypted image is decrypted with ICA algorithm. The analysis results of proposed algorithm compared to existing standard mixing matrix, shows that proposed system facilitates effective and safe way for image encryption.

○ *Image encryption based on chaos with PWL memristor in Chua's circuit:* Zhao-Hui Lin and Hong-Xia Wang [29] introduced a new chaotic image encryption technique. The image encryption algorithm is based on chaos with PWL Memristor in Chua's circuit. Memristor is a non-linear electrical component that forms a relation between electric charge and magnetic flux linkage. The quasi-linear analysis of the circuits with Mermistors is carried out by Piece Wise Linear (PWL) Mermistor model. PWL Memristor is substituted in place of Chua's diode in Chua's circuit. The algorithm contains mainly two processes: image scrambling and pixel replacement. Initially, three chaotic sequences are generated from the chaotic system in the Chua's circuit with PWL Memristor. Secondly, image scrambling is carried out by a random cyclic shifting of rows and columns of image matrix. Finally, pixel replacement is done by applying XOR operation between the sequence *S* and the scrambled image data bit by bit. Decryption process is carried out by calculating inverse of encryption. Proposed algorithm has very large key space and sensitive to key that attackers cannot recover without correct key.

○ *Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination:* Huan Zhang and Ruhua Cai [30] introduced an image encryption algorithm based on combination of bit plane scrambling and multiple chaotic systems. The algorithm can change the grey values of image simultaneously by shuffling its positions. Initially, a grey image is split into many bit planes. Integer sequence is generated based on 4D hyper chaotic system by using Arnold cat map to shuffle the positions of each bit plane pixels. The positions of the rows and columns for each bit plane image are shuffled by generating random integer vector using two dimensional logistic maps. Finally, the scrambled grey image is reconstructed by shuffled bit plane images. This algorithm is resistant to various attacks, poses large key space and key sensitivity, which results in high security.

○ *Efficient image encryption with block shuffling and chaotic map:* Zhenjun Tang, Xianquan Zhang and Weiwei Lan [31] presented this algorithm which mainly consists of three steps: First, initial encryption is carried out by splitting

the original image into overlapping blocks and scrambles the image blocks. Second, a set of secret matrices are generated by using Arnold transform and chaotic map. Finally, XOR operation is applied between elements of random secret matrices and image blocks to obtain final encryption. All steps are controlled by secret keys hence the algorithm is secure and provide large key space. Low complexity computation serves the algorithm to be faster.

○ *Research of image encryption algorithm based on chaotic magic square:* YunPeng Zhang, Peng Xu and LinZong Xiang [32] proposed an image scrambling encryption scheme based on chaotic system. Initially the original image is pre-processed using magic square transformation. In magic square transformation image pixels are transformed into two dimensional matrix *A*, and *A* is multiplied with a sparse matrix *B* to change the rows of the matrix. The resulting matrix is transposed *n* times and saved in another matrix *C*. The pre-processed image is then subjected to Arnold transform (uses keys specified by user) to transposition an image. Two dimensional array and the image scrambling grey values are produced by logistic and Henon mapping. Finally, XOR operation is carried out between the positions transformed image and two dimensional arrays to generate new RGB values resulting in complete encrypted image. The algorithm serves large key space and resistant to attacks.

○ *Digital image scrambling algorithm based on chaotic sequence and decomposition and recombination of pixel values:* Dong Wang et al. [33] introduced this technique. Initially the pixel values of the original image are decomposed into four parts. The new pixels are recombined using logistic chaotic sequence to generate an encrypted image. Logistic chaotic sequence works as defined is previous section. This algorithm scrambles both position and pixel values simultaneously in which the spatial position of pixel can be changed. It diffuses error hence algorithm is secured. It serves large key space, key sensitive, resistant to attacks and is capable of changing grey scale features of images.

• **Summary.** Since a single key is used in symmetric encryption, the strength of encryption relies completely on size of the key used. The algorithm using long key is harder to be cracked than the algorithms using small key. AES is considered to be faster and efficient than other algorithms as it uses variable length of keys and it is standard algorithm used in many applications. Blowfish algorithm has very good performance than other symmetric key algorithms. Blowfish algorithm can even be used as replacement for DES and IDEA. AES have better performance than DES and Triple DES. Triple DES has 1/3 the throughput of DES and it showed poor performance since it consumes more power. RC4 and blowfish consumes more time than other algorithm. Hill Cipher algorithm is not used independently more often, due to lack of security. In the case of encryption with data transmission, there is a significant change in performance of different symmetric key schemes, since most of the resources are consumed for data transmission rather than computation.

2.2. Asymmetric key encryption

Asymmetric key encryption is also called as public key encryption. This approach uses a pair of keys to encrypt and decrypt information for secure transmission.

Initially, a network user will request and receive a pair of keys, i.e., public key and private key from a certified authority. Any other user who wants to send an encrypted data can get expected recipient's public key from public directory. The sender uses this key to encrypt data and sends it to recipient. The recipient receives the ciphered image, decrypts it with their private key. Hence, no one else will have permission to access data other than the intended user.

- ***Rivest-Shamir-Adleman* (*RSA*) *Algorithm*** is proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 to replace a less secure National Bureau of Standards (NBS) Algorithm [34]. The idea behind RSA is motivated by Diffie and Hellman's method of exponential key exchange. RSA is an asymmetric cryptographic algorithm and is one of the strongest algorithms that has never been cracked yet.

The steps in RSA Algorithm are as follows [35, 36]:

Step 1. Generate two large distinct prime numbers p and q.

Step 2. Multiply p and q, assign the value to n ($n = p \times q$).

Step 3. Solve $\varphi(n) = (p-1)(q-1)$.

Step 4. Select an integer e, such that $1 < e < z$ and $\text{GCD}(\varphi(n), e) = 1$.

Step 5. Determine d, such that it satisfies the congruence relation $de \equiv 1 (\text{mod} \varphi(n))$, d is modular multiplicative inverse of e. d is used as private key exponent with modulus n, and e is used as public key exponent with mod$n$.

Step 6. For encryption, $C = P^e (\text{mod} n)$, where C is cipher text and P is plain text.

Step 7. For decryption, $P = C^d (\text{mod} n)$.

Higher the values of exponent more secure the algorithm is. The attackers cannot decompose larger value. The encryption and decryption needs lots of calculations, so the algorithm serves slow of speed. Complex key generation since RSA is limited by efficiency of generating prime numbers. The security of RSA Algorithm would be threatened, if algorithms which can decompose large values come into existence [35, 36].

- *RSA-based digital image encryption algorithm in wireless sensor networks:* Gajendra Singh Chandel and Pragna Patel [37] introduced an algorithm for digital image encryption based on RSA algorithm. Considering the limitations of sensor network resources, a secure transmission based on information hiding for secure data transmission is proposed [34]. The algorithm combines the features of a digital image with RSA algorithm. RSA process mentioned in previous section is used to generate key. This uses the existing wireless sensor networks to transmit the data to obtain low energy cost. This algorithm does not pose the property of anti-attack.

- ***Elliptical Curve Cryptography* (*ECC*)** is an asymmetric key encryption which is introduced by Miller and Koblitz in 1985. Applications of ECC are encryption, digital signatures, and pseudo random number generation. ECC poses same level of security that is provided by RSA, Diffie Hellman but with much shorter keys [38]. The general form of ECC is: $y^2 = x^3 + ax + b (\text{mod} p)$, over a finite field F_p where p is a prime or a prime power, x, y are coordinates and a, b are coefficients (real numbers). The private key d is randomly chosen from $d \in \{1, 2, ..., n-1\}$ where n is the integer, whereas the public key Q is calculated by dP, where P and Q are the

points on elliptical curve. The key pair (d, Q) is used in cryptosystems. ECC provides higher security and it is more efficient than the first generation public key encryption.

○ *DES Algorithm security fortification using elliptic curve cryptography:* Mohamed et al. [39] proposed a scheme, which is a modified version of classical DES algorithm using asymmetric key encryption to overcome liabilities in security issues of DES algorithm. The classical key scheduling of DES is cancelled in this new approach, that is left circular shift operation is cancelled. ECC is used for key generation and distribution to establish a communication session. The algorithm consists of five steps:

Step 1. Both the sender A and receiver B choose a private keys (a&b).

Step 2. Public keys are shared between A and B. It is computed using formula $K_{pubA} = a.G$ and $K_{pubB} = b.G$, where G is base point.

Step 3. Retrieve joint secret $T_{AB}=b.K_{pubA}$ and $T_{AB}=a.K_{pubB}$, this will produce same value. Locate point on the curve $T_{AB} = (x_{AB,} y_{AB})$, where x_{AB} and y_{AB} are 192 bits, since curve is P-192 (prime field).

Step 4. Obtain another point on Elliptical Curve (EC), A and B calculates $2T_{AB} = (x_{2AB,} y_{2AB})$ which is double of join secret. The entity has two points on EC (T_{AB}, $2T_{AB}$).

Step 5. A and B merges four coordinates $x_{AB,} y_{AB,} x_{2AB,} y_{2AB}$ (binary format 4×192 bits) to obtain 768 bits that is input (16×48 bits) for DES encryption. The output of Step 5 is reformed into matrix structure of 16×48 bits. Thus each row is a round key, that 16 sub keys of DES's round. DES is performed for encryption and decryption. This new method can also be used in encryption of any file format. The method possesses a very large key space to resist the brute-force attacks and it is more secure. The proposed method is very immune to statistical attacks.

○ *Encryption of image matrix using elliptic curve cryptography:* Suganya and Sathiya [40] introduced an image encryption techniques based on elliptic curve cryptography. In this proposed scheme, each value of the input data is transformed into elliptic curve points (X_m, Y_m) and these point are then converted into a cipher. The proposed encryption algorithm initially generates EC coordinates in a finite field p with given parameters A, B. Convert the data to obtain coordinates on EC $F_p(A, B)$. Select a base point G from the generated EC. Perform point multiplication on G by k times G to obtain first encrypted point. Apply point multiplication on public key of B. Obtained value is then added over the point corresponding to the message P_m. The result generated is the second point of encrypted message. Transmit the two encrypted points. During decryption the message m is converted into EC coordinates as $X_m = m*k+j$, where k is random integer and j is iteration value. The first point is subtracted from second point N_b (private key of B) times. This proposed method uses less computation compared to other algorithms such as RSA.

2.2.1. Recently proposed asymmetric image encryption methods

○ *Asymmetric image encryption based on matrix transformation:* Yang Shuangyuan, Lu Zhengding and Han Shuihua [41] proposed a novel asymmetric block encryption scheme. Mainly used for large amount of data. It also

shows how to adapt certain matrix transformation for encryption. Initially, a pair of keys is produced by matrix transformation and then image is encrypted in its transformation domain. Pair of keys are generated by two matrices (U and V) and created with Gaussian white noise and U and V are multiplied each other to obtain invertible matrix A. S is the principal square root of A. VS^{-1} and $S^{-1}U$ are the private and public key pairs. The encryption algorithm divides the input into $P \times P$ blocks and is transformed into Discrete Cosine Transform (DCT) domain. DCT is mainly used in image compression technique which converts signal into elementary frequency components using simple computational functions. Use private key to encrypt frontal $K \times P$ coefficients of each block. Perform inverse of DCT and combine all $P \times P$ blocks to obtain encrypted image. Decryption is inverse process. Several attack analysis are done. This approach provides good security and less computational complexity.

○ *New hybrid asymmetric key-exchange and visual cryptographic algorithm for securing digital images:* K e s t e r, N a n a and P a s e u [42] proposed an asymmetric technique on digital image using hybrid method. Two parties in communication exchange the public key. Public key is generated by randomly chosen private key with forward hashing function algorithm. Exchanged keys are used for encryption. The encryption algorithm computes the shared key by using public key and private key. Represent input image pixel into a matrix. Get width c and height p of input image. Shared key is used in every shift of share of input image. Remove red component as a share r, green component as g and blue component as b. Let r', g', b' be the transpose of r, g, b. Resize r', g', b' into (r, c, p), (g, c, p) and (b, c, p). Merge the r', g', b' into same size of r or g or b of input image. Convert the data into image format to obtain encrypted image. This approach produces an effective implementation on requirements such as confidentiality, integrity, authentication and non-repudiation.

○ *Heuristic approach for secured transmission of image based on bernstein polynomial:* S m i t h a S a s i and S w a r n a J y o t h i [43] introduces an efficient algorithm based on Bernstein polynomial over Galois Field GF(p). Bernstein polynomial is linear combination of Bernstein basis polynomials. The equation for polynomial in Bernstein form of degree n is

$$n(f,t) = \sum_{r=1}^{n} \frac{1}{n} nc_i t^i (1-t)^{(n-i)}, \tag{5}$$

where nc_i is binomial coefficient and the exponent on the $(1 - t)$-th term decrease by one as i increases. Polynomial with degree n=5, is called quintic polynomial. Compute (x, y) coordinates based on degree of polynomial and image for Bernstein coordinate elements is obtained. This approach uses Bernstien image to compress input image and then compressed image is encrypted using proposed algorithm. During compression the input is divided using Bernstein image. The encryption uses a pair of keys (K_u, K_r) to find secret reference value K in the curve based on quintic polynomial. Perform $a=(P/K_u)(\text{modGF}(p))$, where $p=n^2+n-4I$, P is the pixel values of compressed image, $a=P+n(K_u-P)(\text{modGF}(p))$. Finally, perform $(a/K)(\text{modGF}(p))=C$ to obtain encrypted image where $C=a+n(K-a)(\text{modGF}(p))$. Decryption performs $(a_1/K_r)(\text{modGF}(p))=P$, where $P=b_1+1/n(K_r-b_1)(\text{modGF}(p))$ to obtain compressed pixel values. Relation between K_u and K_r is obtained by:

$K_r = n[(b - nK_u)/(1-n) + b(1-n)/n] (\mathrm{mod} p)$. The decrypted image will be decompressed to obtain the input image. This scheme has lower process time and thus reduces computational complexity.

o *New method of generating public key matrix and using it for image encryption:* Sukant Chhotaray, Animesh Chhotaray and Girija Rath [44] presented a new technique to generate self-invertible matrix, generate sparse matrices based on a polynomial method and the steps in inversion of this matrix without using standard matrix inversion algorithm. The self-invertible matrix B (2×2 size) in which partition matrices B_{11}, B_{12}, B_{21}, B_{22} are generated using another matrix A ($m \times m$ size) by the relation: $B_{11}=A^3$, $B_{22}= -A^3$, $B_{12} \times B_{21}=I - A^6$. The sparse matrix S is generated using Eigen function: $f(\lambda) = \lambda^n + s_{n-1}\lambda^{(n-1)} + ... + s_0 = 0$. The individual matrix servers as private key and the product of two matrices are used as public key. The self-invertible and the sparse matrix will be known. The encryption is done with public key C, generated using key matrix A and B where $C = ABA$. During encryption input image is divided into 8×8 blocks. Each block is encrypted using C and all blocks are combined to obtain encrypted image. The inverse of B is found by relation $BB^{-1} = I$ and inverse of C is generated by relation: $D=AB^{-1}A$. Decrypt the blocks using D. In comparison of the proposed algorithm with AES. Analysis shows very low computational complexity and reduced brute force attack.

• **Summary.** Asymmetric algorithm uses a pair of keys, one for encryption and one for decryption so it provides better security when they transmit data over a network. Most of Public key algorithms are established based on some number theoretic functions that require arithmetic with long operands and keys. Longer the keys and operands more secure the algorithms is. RSA is the best known algorithm, which poses strong security hence it can be used for encryption of long messages without employing the hybrid and symmetric encryption. RSA key generation takes more time for calculation, thus it serves very slower. ECC poses same level of security with much smaller keys, therefore it consumes less computing power, memory and time. ECC requires low processing overhead than that of RSA. There is an increase in size of the encrypted messages using ECC than that of RSA. ECC is more difficult to implement, increasing the likelihood of error in implementation hence reduces the security of algorithm.

2.3. Properties of a good key based Image encryption schemes

This section discusses certain parameters that can be used to evaluate the efficiency and security of an image encryption scheme.

• ***Correlation coefficient*** is a useful measure to evaluate encryption quality of any cryptosystem [45]. The goodness of cryptosystem depends on ability of encryption algorithm to hide all the attribute of input image and ciphered image which is totally random and uncorrelated [45-47]. Correlation computes degree of similarity between two variables [48]. If ciphered image and input image are completely dissimilar, then their corresponding correlation coefficient must be very low, or very close to zero. If ciphered image and input image are totally similar, then their correlation coefficient is equal to 1 (perfect correlation). If ciphered image is negative of input image, the correlation coefficient is –1. Image encryption process

completely fails when correlation coefficient is 1, because ciphered image and input image completely identical. The Correlation Coefficient (CC) is calculated as in (6), where x and y values of two pixels in the same position of input image and encrypted image, Cov is covariance at pixels x and y. σ_x, σ_y is the standard deviation which can be calculated as, $\sigma_x = \sqrt{\mathrm{VAR}(x)}$, $\sigma_y = \sqrt{\mathrm{VAR}(y)}$ where VAR is the variance at each pixel (x and y). E is the expected value operator and N is the total number of pixels in $N \times N$ matrix.

$$C.C = \frac{\mathrm{Cov}(x, y)}{\sigma_x \times \sigma_y},$$

$$\mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{6}$$

$$\mathrm{VAR}(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^i.$$

• ***Histogram analysis.*** In statistics, histogram is a graphical representation of data distribution. The total area of the histogram is equal to the number of data. An image histogram is a total distribution in a digital image by plotting the number of pixels for each tonal value. An image encryption algorithm is considered "ideal" if encrypted image has uniformly distributed histogram. Consider for instance Fig. 3 and Fig. 4, it is clearly shown that the histogram of the encrypted image is nearly uniformly distributed and significantly different from secret image. Thus, we may conclude that the encrypted image does not provide any clue to employ any statistical attack.

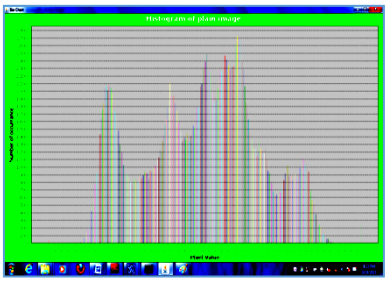


Fig. 3. Histogram of secret image

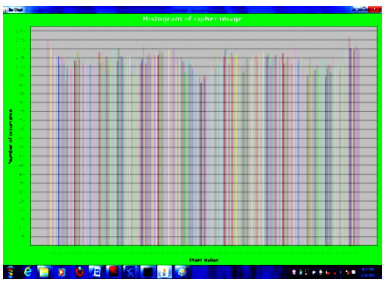


Fig. 4. Histogram of encrypted image

• ***Lossless information.*** The difference between the pixel values of input image and the corresponding pixel values of encrypted image may be calculated to prove that, there is no loss of information. If the difference between input image and the encrypted image is always 0 for all pixels, then there is no loss of information. Fig. 5 shows an example of difference between pixels of secret image and the pixels of encrypted image. This property can also be confirmed by plotting the values obtained in a histogram. Fig. 6 shows the histogram of Fig. 5.

Fig. 5. Difference output

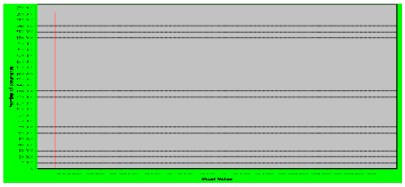


Fig. 6. Histogram of Fig. 5

• ***Avalanche effect*** is very important property of any cryptographic algorithm. This concept results in significant change of cipher text image when there is a small change in key or plaintext image.

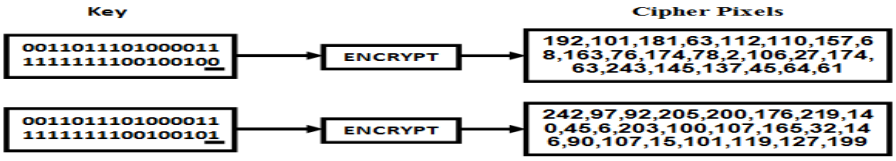


Fig. 7. Avalanche effect

Strict avalanche effect occurs when a single bit change in the plaintext image changes complete half the bits in cipher text image [48]. Fig. 7 exhibits an example of avalanche effect; a single bit change in the initialization vector of feedback shift register will produce entirely different cipher pixels. It is a desirable property of all cryptosystems

• ***Information entropy analysis*** is a measure of uncertainties or random events in any communication system. This concept is very important for analysing an encrypted scheme and also useful in lossless data compression, statistical inference, cryptography. The concept of information entropy is proposed by Claude Elwood Shannon which describes that information theory is mathematical theory of storage and data communication [49]. The entropy $H(m)$ of message can be calculated as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)}, \tag{7}$$

where $p(m)$ is the probability of occurrence of symbol m_i.

• ***Compression friendliness*** is one of the basic requirements of image encryption. Very large multimedia data can be compressed by entropy based coding algorithms. Multimedia compression is very useful procedure before and after encryption or during encryption [50]. Since compression eliminates regular patterns from plaintext, it may overcome the problem of statistical attack. Compression can also reduce storage space and transmission bandwidth; hence it has a vital role in the field of cryptography. Compression before encryption is most advantageous than after encryption. Various compression coding methods have been introduced on entropy theory such as arithmetic coding, run length coding [50].

• ***Encryption quality*****.** Evaluation of quality of image is an important issue in image encryption algorithm. An image encryption algorithm is judged based on its ability to conceal a large number of image features. There are certain parameters to express the quality of the encryption [51, 52]. *Maximum deviation:* The quality can

be accessed by measuring maximum deviation in pixel values between the plaintext image and ciphered image. *Irregular deviation:* Measures the amount of statistical distribution of histogram deviation is close to uniform deviation. The encryption quality is fit if irregular deviation is close to uniform deviation. *Peak Signal to Noise Ratio* (*PSNR*): Measures the changes in pixel value between plaintext image and ciphered image [53]. PSNR is an effective method to measure quality.

- ***Effect of Noise.*** A good image encryption algorithm should work in noisy environment and must be robust against noise. Noises with different Signal to Noise Ratio (SNR) are used on ciphered text to test immunity. Algorithm must be capable of noise resistance.
- ***Key sensitivity analysis.*** A good image encryption algorithm should be very sensitive to key that is used. High key sensitivity is required by secure image cryptosystem which means the encrypted image cannot be decrypted correctly even if there is a small difference between the encryption and decryption keys.

3. Image encryption without key

Image encryption without key is a technique which provides information security which uses simple algorithm where no mathematical computation is required. Fig. 8 clearly depicts image encryption process. In this technique a secret image is split into random shares using image Encryption schemes. Stacking these shares reveals the secret image. Shares are usually presented in transparencies.

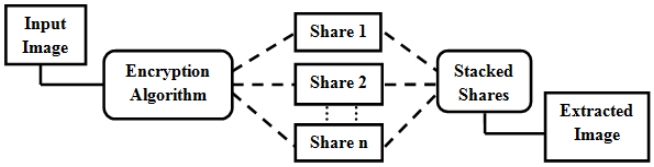


Fig. 8. Image encryption without key

Visual Cryptography Scheme (VCS) uses one of the following access structures for its implementation [54]:

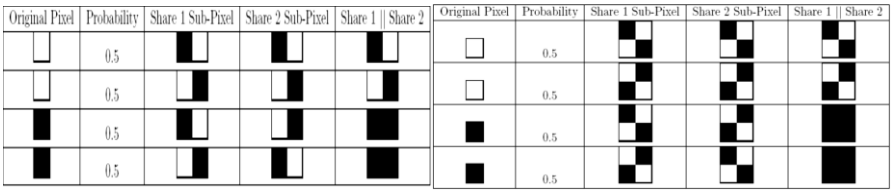
- (2, 2) VCS: One of the simplest VCS where secret image is encrypted into exactly 2 shares. The secret image is recovered by overlaying two encrypted shares.
- (2, *n*) VCS: The secret image is encrypted into *n* shares and when any two (or more) shares are overlaid the secret image can be recovered.
- (*n*, *n*) VCS: The secret image is encrypted into *n* shares and it can be recovered only when all *n* shares are overlaid.
- (*k*, *n*) VCS: The secret image is encrypted into *n* shares and when *k* shares are combined secret image can be recovered.
- Image encryption without key can be further traditional share generation and random grid approach.

3.1. Traditional share generation

In traditional share generation scheme, an image is split into n shares where all n shares are essential to decrypt the image. Any $n-1$ shares can recover no information about the original image. The decryption of an image encrypted by this scheme requires no mathematical computations or knowledge of cryptography. Each share is written on a separate transparency, and decryption is performed by overlaying the share. Each pixel of the input image is placed with 2 or 4 pixels in share. Hence, size of generated share is larger than input, possibility of pixel expansion in overlaid image is high. The aspect ratio of the input will be distorted in the decrypted version due to assignment of 2 sub-pixels for one original pixel is double the width of the decrypted image while recovering its original height.

- **2 out of 2 algorithms.** The first VCS scheme coined by Naor and Shamir [55]. They proposed 2 out of 2 algorithm, during encryption 2 shares are generated ($n = 2$) from original image, decryption requires exactly these 2 shares ($k = 2$) to be super-imposed. This algorithm works by representing each pixel of the original image by 2 pixels in each share. Read each pixel in the original image, when a white pixel is encountered, one of the first two rows of Fig. 9a is chosen with equal probability, and assigns each share with 2 pixel block as shown in the third and fourth columns. When a black pixel is encountered, one of the last two rows is chosen with equal probability, and a sub pixel is assigned to each share.

During decryption, superimposition of shares works similar to Boolean OR function. If two white pixels of corresponding shares overlap, the resulting pixel will be white. When a black pixel in one share overlaps with either a white or black pixel in the other share, the resulting pixel will be black. The last column in Fig. 9a shows the resultant sub pixel when the sub pixels of both shares in the third and fourth columns are superimposed. The main issue with this algorithm is, superimposed image appears distorted due to the fact that the use of 2 sub-pixels for each original pixel doubles the width of the superimposed image when overlaid.



(a) (b)

Fig. 9. 2 out of 2 using 2 sub-pixels (a); 2 out of 2 using 4 sub-pixels (b)

To solve issue of distortion of the aspect ratio of the original image, Naor and Shamir [55] suggested using a 2×2 sub-pixel block to represent each original image pixel. This generates an image that is four times the size of the original image, but retains the aspect ratio of the original image producing a clearer and more natural looking result. Fig. 9b shows the 2×2 sub-pixels used in 2 out of 2 algorithms.

3.1.1. State of art of traditional share generation methods

○ *Visual Cryptography:* Naor and Shamir [55] introduced a Visual Cryptographic Scheme without using any cryptographic computations. This scheme is an extended visual cryptography as a visual variant of the *k* out of *n* secret sharing problem. In a secret sharing scheme, one wishes to divide a secret amongst a group of *n* individuals called shares in such a way as to allow any $k < n$ of them (or, in certain cases, only a qualified subset of them), to reveal the secret from their individual shares. This scheme is simple and easy to implement.

○ *Novel image secret sharing scheme:* Prabir et al. [56] presented a scheme which is implemented using a simple graphical masking, by applying simple AND operation for share generation and recovering is done by simple OR operation on a set of shares. Masking algorithm to produce mask for *n* shares with threshold *k* works in two stages: First the algorithm lists the *n* number of row vectors having combination $k - 1$ number of zeroes and $n - k + 1$ number of 1s and assign them to a matrix of dimension ${}^{n}C_{k-1} \times n$. Secondly, transpose the resultant matrix to dimension $n \times {}^{n}C_{k-1}$. Each row of the matrix will be mask for each *n* shares. The algorithm constructs a secret share, the image is encrypted and ciphered image is shared and is compressed. The compressed shares lead to strong security of the secret image. The header share is constructed with six fields: total number of shares *n*, threshold *k*, encryption key *K*, input image of width *w*, padding bits *p*. The original secret image is reconstructed using appropriate masks to obtain expanded secret share and then OR operation is performed on *k* number of secret share to obtain reconstructed encrypted image. Confidentiality and Integrity are main benefits of this scheme.

○ *Enhancement of security in visual cryptography system using Cover Image Share Embedded Security Algorithm* (*CISEA*)*:* Himanshu Sharma, Neeraj Kumar and Govind Kumar Jha [57] proposed CISEA to produce shares from the input image. This scheme introduces a new concept for generation of compliment images of a cover image over which the shares of input image are to be mapped. The proposed algorithm works with three phases: Phase 1: The original image *I* is converted into binary image *S* using any halftone technique (this technique converts grey scale image into binary). Shares S_1 and S_2 are generated using traditional share generation approach described in previous section. Phase 2: Four embedded images X_{11}, X_{12}, X_{13}, and X_{14} are generated using a cover image *C* and its complimented images C_1 and C_2. Embed S_1 and S_2 over C_1 and C_2 as: X_{11}=embedded(S_1, C_1); X_{12}=embedded(S_1, C_2); X_{21}=embedded (S_2, C_1); X_{22}=embedded(S_2, C_2). Due to generation of C_1 and C_2 an additional security is provided by digital watermarking scheme, is a technique that embeds a secret image onto a cover image to maintain the quality of secret image. Resultant image of this phase is encrypted image. Phase 3: Decryption phase: decryption is carried out using traditional share generation to recover image at receiver's side. CISEA provides one more layer of security for the images in communication network and facilitates improved security.

• **Summary**: Visual cryptography scheme is applicable only for the data in image format. VCS avoids complex computation issues in decryption process by restoring the input image by stacking operation. This property is very useful for

application having low computation resources. Traditional Share Generation approach is a simple and secure method which encrypts an image by generating shares and decrypts directly during human vision. Factors that can affect the quality of the resulting decrypted image in a VCS are pixel expansion and contrast of reconstructed image. The contrast of the resulting decrypted image worsens in terms of distorted aspect ratio due to increase in the number of shares *n*. Furthermore, pixel of the original image is represented by multiple pixels in each share, diminishing the resolution of the decrypted image resulting in pixel expansion. To solve this problem VCS based on random grids are introduced.

3.2. Random grid

This is an advanced technique of traditional share generation approach; the size of generated image is similar to input image. Random Grid (RG) technique is to encrypt input without pixel expansion. This technique takes an input image and splits into multiple cipher-grids that hide information of the input image. Each pixel of the input is placed with exactly 1 pixel in share. Hence, they require no pixel expansion, and therefore each share retains the size of the input image. The following section describes the two techniques using RG.

- **2 out of 2 using random grids.** K a f r i and K e r e n in [58] proposed 2 out of 2 VCS based on RG. The technique uses two reference images R_1, R_2 (like in Fig. 10) and an input image *I* of similar sizes. R_1 contains randomized black and white pixels. R_2 is constructed by reading *I* at position (*x*, *y*).If the pixel is white than the R_2 at location (*x*, *y*) contains same pixel as in R_1 at location (*x*, *y*).In contrast if the pixel at location (*x*, *y*) is black than the R_2 at location (*x*, *y*) is set to opposite of R_1 at same location (*x*, *y*). Fig. 10 shows the representation of pixels in each transparency based on a pixel corresponding to input image. The transparencies are superimposed using Boolean OR operation. This method can only decrypt 50% of the white pixels of *I*. If the number of white pixels in *I* is more, than this technique may not reveal *I* with high contrast. This method works fine when there is even distribution of black and white pixels.

$I[x,y]$	$R_1[x,y]$	$P(R_1[x,y])$	$R_2[x,y]$	$R_1[x,y] \| \| R_2[x,y]$
		0.5		
		0.5		
		0.5		
		0.5		

Fig. 10. Pixel table for Kafri-Keren Algorithm

- ***n* out of *n* using random grid.** Chen and Tsao (see [59]) proposed an *n* out of *n* RG algorithm based on Kafri-Keren Algorithms [58], where any number of shares can be generated for a given input image provide all shares must be superimposed to decrypt image. The algorithm creates a chain of cipher-grids, where each successive cipher grid can decrypt the previous one. Therefore, when all cipher grids are superimposed, original image can be recovered.

Initially the algorithm creates R_1 and R_2 from the original input image using the Kafri-Keren Algorithm where R_1 will be selected randomly and R_2 is generated based on the pixels of R_1 and I.

3.2.1. Recently proposed random grid image encryption method

- *Flexible multiple-secret image sharing scheme by shifting random grids:* Ming-Jheng Li and Justie Su-Tzu Juan [60] introduced this technique which is an extension to Multi VCS proposed by Chang and Juan (see [61]), the scheme works by encrypting three secret Images into two Shares by shifting Random Grids (called as ISRG scheme). In their technique the distortion of the secret image is same, therefore in order to make the distortion more flexible this paper proposed a scheme where distortion of the last secret image can be selected flexibly and can be used more practically and flexibly. This paper proposed a new flexible multiple-secret image sharing scheme by shifting random grid (called *R*-Algorithm) in which distortion can be flexibly selected. *R*-Algorithm let S_k be a secret image in which k is the number of secret images, initially selects a secret image S_1 that is not equal to S_2 randomly.
- *On multi-secret sharing using Hill cipher and random grids:* Jothi and Ojha [62] proposed this method. The scheme is an addition to visual secret sharing scheme for grey scale images introduced in by Chen [63], includes two steps in encryption: initially, the original image is divided into two equal sized pixel blocks and pixels from each block is encrypted using Hill cipher. Secondly, the sub images obtained from Step 1 are translated into two cipher grids by applying bit wise XOR operation between sub images and a RG. This scheme uses same method, but pixels from two secret images are considered to build pixel blocks and then encrypt into cipher grids through Hill cipher (as described in previous section), and then the RG in the second layer provides additional security. The main advantage of proposed scheme is high security with lossless image recovery and no pixel expansion.
- *Random grid based visual cryptography using a common share:* Sruthy and Ramesh [64] proposed a visual cryptography technique using RGs, where it uses a common share to transfer *n* binary secrets. The binary secret image is split into two shares by RGs similar to (2, 2) VCS. This scheme use n+1 share images to transfer n secrets and the addition share is common to all n secrets. This scheme can be considered as an extension of (2, 2) RG VCS. Efficient network bandwidth utilization achieved by considering one share as a common share to all n secrets.

- **Summary.** RG is a transparency of pixel with two dimension where each pixel may be completely transparent (white) or totally opaque (black). A binary input image is encrypted into two noises like transparencies of same size as that of the input image and these two transparencies are stacked to recover the original image. One of the major advantages of RG over basis matrices is that size of generated image is unexpanded. RG scheme is similar to probabilistic model of the VCS but RG is not based on basis matrices. Kefri and Keren's RG scheme solves the requirement of pixel expansion problem which is proposed prior to Naor and Shamir approach.

3.3. Extended visual cryptography

Extended Visual Cryptography Scheme (EVCS) is different from previous schemes in the sense instead of creating random or meaningless shares, it generates meaningful shares. If these shares are stacked together than meaningful share disappears and secret image is revealed.

- *Embedded EVCS:* L i u and W u [65] introduced an embedded EVCS which embeds random share into meaningful covering share. The proposed schemes works mainly in two stages: Stage 1 – generate *n* number of covering shares by using *n* input original share image, and Stage 2 – embeds the corresponding VCS into *n* number of covering shares to generate embedded shares. Stage 1, outputs *n* binary meaningful shares where information of patterns in the original share are all covered and produce black images when qualified shares are stacked. Halftone technique or dithering technique is the process used to convert the grey scale image to binary image. Halftone technique by using dithering matrix is carried out. Dithering matrix denoted as D is a $c \times d$ integer matrix which holds grey levels of pixels. The position of dithering matrix is represented as the universal set $\mathcal{G} = (g_{0,}\, g_{1,\ldots,}\, g_{h-1})$, where h is halftone pixel expansion. The construction of *n* covering shares takes place in three steps. Initially, covering subsets (A_0, A_1, ..., A_{n-1}) as *n* subsets of $\mathcal{G}$ with minimum Average Black Ratio (ABR) is generated first for threshold access structure called threshold covering subset. The black ratio is defined as $R(A_i, \mathcal{G}) = |Ai|/|\mathcal{G}|$, and the ABR is defined as $\bar{R}(A_i, \mathcal{G}) = (\sum_{i=0}^{n-1} |A_i| / (n|\mathcal{G}|)$.It is then extended to general access structure called general covering subset. Secondly, resulting subsets are converted into dithering matrices (D_0, D_1, ..., D_{n-1}) by starting with a random matrix which contains grey levels. Finally, covering shares (s_0, s_1, ..., s_{n-1}) are generated from original share images (I_0, I_1, ..., I_{n-1}) using dithering matrices. Stage 2, the embedding process. This process first make use of corresponding VCS to encrypt a secret image I to (C_0, C_1) shares with pixel expansion m and then embeds the shares generated by VCS into resulting covering shares of stage. Embedding process is carried out in four steps:

Step 1. Divides the covering share into blocks where each block holds t ($\geq m$) sub-pixel.

Step 2. m embedding positions in each blocks are selected.

Step 3. Randomly choose a share matrix $M \in C_1$ for each black pixel in I (respectively white, $M \in C_0$).

Step 4. m sub-pixels of each row of M is embedded into the selected m embedding positions in Step 2. The pixels in the embedding positions are replaced by sub-pixels of M.

While stacking the embedded shares the $t - m$ pixels that have not embedded will always appear black and m sub-pixels that are embedded in Stage 2 will recover the secret image. When image I is smaller than covering image, the value t may have number of choices. While t is larger, we may have more sub-pixels $t - m$ hiding the information of covering shares and when m is larger, D can simulate more grey levels resulting in better visual quality of the shares, thus the proposal is flexible with share pixel expansion, secret image pixel expansion and visual quality of the image.

- *EVCS without pixel expansion for halftone images*: Askari, Heys and Moloney [66] presented a scheme based on EVCS. The scheme processes halftone image which improves the quality of the share image as well as the recovered secret image. The paper proposed a novel and effective balanced block replacement (BBR) method for replacing the candidate blocks of a halftone secret image. BBR approach balances white and black in the processed image by assigning some candidate blocks to black and others to white. The block of 2 white and 2 black pixels is known as candidate block. Generation of grey scale image for VCS is carried out in three steps.

Step 1. Transform grey scale image into halftone image. Split the halftone image into non overlapping blocks (2×2 pixels). Divide the halftone image into overlapping squares of four 2×2 blocks where each grouping of four blocks is called as a cluster.

Step 2. Count and save the number of black pixels in each cluster of halftone image in a template which is used as the threshold value of the cluster. Classify all secret blocks which hold one black (respectively white) pixel and covert the secret block with one black (respectively white) to white (respectively black) block. The resulting image is initial processed image.

Step 3. The processing starts from the first top left block of the cluster of initial processed image and moves to left-right: top-down in a raster format. The number of black and white pixels in each cluster of initial processed image is kept as close as possible to the threshold value of the cluster of the original halftone image. While candidate block is converted to black block 2 pixels are added to the number of black pixels in a cluster and while candidate block is converted to white block 2 pixels are deducted from the number of black pixels from a cluster. This conversion is made in order to match smallest difference between threshold and the number of black pixels in the image being processed.

The proposed methods keeps number of black and white pixels in each cluster of processed image close to threshold value of original halftone image. Thus, the quality of the resulting recovered image is closer to the original grey scale image.

- *Colour EVCS Using Error Diffusion:* Inkoo Kong et al. [67] proposed coloured EVCS using Visual Information Pixel (VIP) synchronisation and error diffusion half toning. Error diffusion is an efficient method for generation of halftone image where it filters quantization error at each pixel and feeds it back as future input. Visual contrasts of shares are improved by VIP synchronization across the colour channels. This prevents degradation of colours and contrast of original shares even with matrix permutation. Each colour channel (Cyan *C*, Magenta *M*, and Yellow *W*) has only one bit per pixel to recover colours of original share since halftone process is applied independently to each colour channel. The proposed method is carried out in two steps.

Step 1. Derivation of the matrix from a set of standard VC and this matrix is used in VIP synchronization. A set of basis matrices $S_c^{c_1,c_2,\ldots,c_n}$ (c_1, c_2, ..., $c_n \in \{0, 1\}$) are generated where c is pixel bit from secret information and c_1, ..., c_n is the corresponding pixel bits from the shares. VIPs are pixels that hold colour information of the original shares. There are q numbers of VIPs (expressed as c_i) in each row of $S_c^{c_1,c_2,\ldots,c_n}$ and the values in the matrix derivation stage are unknown. The actual bit

value of c_i is defined by halftone processing by referring the pixel values of original share and error diffused away.

Step 2. Error diffusion method to generate final share. In this process the quantization error at each pixel is used as feedback input. Each of the three colour layers is fed into the input to generate the *i*-th halftone share. The error filters are implemented in such a way that it produces pleasing halftone image for human vision by minimizing low frequency difference between the input and output image.

The difference between standard error diffusion and proposed error diffusion method is that the components of secret information are predefined on the input share and it remains same during the halftone process.

• **Summary.** EVCS as opposed to traditional VCS keeps meaningful information in share instead of random noise. If these encoded shares are transmitted through network; an attacker will see some false meaningful information. We conclude that EVCS scheme does not give any clue that some information is encrypted in the corresponding shares.

3.4. Properties of a good keyless image encryption scheme

• ***Distortion of image.*** Normally if the size of the recovered image is expanded *n* time ($n \geq 1$) than its original image and while *n* is not a square number, results in distortion. This is the most common issue in VCS. The aspect ratio of the original image will be distorted if the Decrypted version of the image use *m* ($m \geq 1$) sub pixels per original pixel doubles the width of the secret image while retaining its original height. Several VCS have been proposed in order to obtain a non-distorted image such as fountain algorithms, improving the quality of the image. An ideal VCS scheme results in non-distorted image.

• ***Alignment of image* (*pixel expansion*).** This property deals with alignment of the sub-pixels in the transparencies. If size of the sub-pixel is larger it is easier to align, but the size of the transparencies will be very large. If size of the sub-pixel is smaller it is hard to align, but size of the transparencies will be small. Transmission becomes much easier if the size of the transparencies is smaller. Pixel Expansion is one of the major issues with sub-pixel alignment. Solution to this problem, i.e. to reduce pixel expansion is to reduce the number of the sub-pixel that replaces the pixel of original image. RGs share generation method in visual cryptography is mainly introduced in order to reduce pixel expansion. The size of the transparencies is not only affected by the number of sub-pixels but also by size of the sub-pixel. The size of transparency is equal to the product of number of sub-pixels in transparency and size of the sub-pixel. A good VCS will have smaller transparencies and easily aligned shares. The transparencies need not be aligned precisely to recover the original image.

• ***Thin line problem.*** It is a most common problem that arises in secret image where each pixel in the original image is encountered, it is placed with equal probability, and each pixel is assigned to two or more pixel blocks. While recovering the secret image, thin lines are usually unclear and misplaced in recovered image causing Thin Line Problem (TLP). TLP are categorised in three ways:

1) The quality of the recovered image is degraded by chaotic pixels in such a way that it is difficult to identify the thin lines present in the original image.

2) Some part of thin lines will be clearly visible. Possibility of the line patterns in the secret image is falsely recovered, where the pixel blocks of a thin line in the share generation will be placed in such a way that the thin line may be missing if it is a black (resp. white) thin line on the white (resp. black) background.

3) Thin line will be represented by thicker line in the recovered image.

- ***Visual cheating prevention.*** *W*hen a cheater assigns a fake share during the reconstruction phase which is stacked with the few genuine shares which reveals a superimposed fake image. A participant who does not get the fact of being fooled and believes that the recovered image is an original image is called a victim. A cheater will know basic matrices. A good VCS must be immune to cheating. Various Cheating Immune Visual Cryptography Schemes (CIVCS) are proposed. The main ideas behind these techniques are: to verify the validity of the shares that are stacked by seeking help with an online trusted authority, verify the validity of the stacked shares by generating the extra verification shares, homogeneous secret images must be encrypted using genetic algorithms, possibility of cheaters assumption on share distribution must be reduced by generating more than *n* shares, to add authentication information by expanding the pixel expansion schemes.
- ***Flipping of image in VCS.*** Flipping in VCS is the direction and the order in which each shares must be stacked to recover an original image. Any change in direction or the order of the shares while stacking must not reveal original image.

4. Conclusion

This paper focuses on various Image Encryption schemes (key and keyless). The detailed survey of each technique has been presented and it clearly shows that each image encryption technique has its own unique feature. Basic requirements of Image Encryption are presented in brief. The various properties of a good encryption algorithm (both key and keyless) are described. Image encryption with key(s) provides strong security due to use of key(s) in encryption, but key generation and distribution is most tedious task. The entire process can be compromised if key(s) or Initialization Vector (IV) is revealed. The solution for this key distribution problem may be the use of Visual Cryptography schemes. To sum up, both the Key(s) and Keyless Approaches are useful in real time encryption of image application. Both of the techniques has its benefits and liabilities. There are several properties to be a considered for designing an ideal image encryption algorithm, thus it is a challenge for any researcher to design and maintain a good encryption scheme.

References

1. Stallings, W. Cryptography and Network Security. 5th Edition. Pearson Publishers, Prentice Hall, 2011.
2. Salama, D., A, Minaam, H., M. Abdual-Kader, M. Mohamed Hadhoud. Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types. – International Journal of Network Security, Vol. **2**, 2010, No 2, pp. 78-87.

3. G o n g-B i n, Q., J. Q i n g-F e n g, Q. S h u i-S h e n g. A New Image Encryption Scheme Based on DES Algorithm and Chua's Circuit. – In: Proc. of IEEE International Workshop on Imaging Systems and Techniques, 2009, pp. 168-172.
4. L i n g, B., L. L i c h e n, Z. J a n. Image Encryption Algorithm Based on Chaotic Map and S-DES. – Advanced Computer Control (ICACC), IEEE, Vol. **5**, 2010, pp 41-44.
5. K a u f m a n, C., R. P e r l m a n, M. S p e c i n e r. Network Security: Private Communication in a Public World. Upper Saddle River, NJ, US, Prentice Hall Press, 2002.
6. N i e, T., T. Z h a n g. A Study of DES and Blowfish Encryption Algorithm. – In: Proc. of TENCON-IEEE Region 10 Conference, 2009, pp. 1-4.
7. X i a o, H., Q. S h u i s h e n g, D. C h e n g l i a n g. A Composite Image Encryption Scheme Using AES and Chaotic Series. – In: Proc. of 1st ISDPE, IEEE, 2007, pp. 277-279.
8. M s o l l i, A., A. H e l a l i, H. M a a r e f. Image Encryption with the AES Algorithm in Wireless Sensor Network. – In: Proc. of 2nd International Conference on Advanced Technologies for Signal and Image Processing, IEEE, 2016, pp. 41-45.
9. S c h n e i e r, B. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). – In: Proc. of International Workshop on FSE, Springer, Vol. **809**, 1994, pp. 191-204.
10. A u r o r a, T., P. A r o r a. Blowfish Algorithm. – IJCSCE, Vol. **2**, NCRAET-2013, Special Issue, pp. 238-243.
11. A l i, M., B. Y o u n e s, A. J a n t a n. Image Encryption Using Block-Based Transformation Algorithm. – IAENG International Journal of Computer Science, Vol. **35**, 2008, No 1, pp. 407-415.
12. R i s e, R. E., S.-H. C h o, D. K a y l o r. RC4 Encryption. 2008. **https://www.math.washington.edu/~nichifor/310_2008_Spring/Pres_RC4%20Encryption.pdf**
13. S t o š i ć, L., M. B o g d a n o v i ć. RC4 Stream Cipher and Possible Attacks on WEP. – IJACSA, Vol. **3**, 2012, No 3, pp. 110-114.
14. M o u s a, A., A. H a m a d. Evaluation of the RC4 Algorithm for Data Encryption. – International Journal of Computer Science and Application, Vol. **3**, 2006, No 2, pp. 44-56.
15. G i n t i n g, R. U., R. Y. D i l l a k. Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map. – ICITEE, IEEE, 2013, pp. 101-105.
16. S a s i d h a r a n, S., D. S. P h i l i p. A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4. – International Journal of Advances in Engineering & Technology, Vol. **1**, 2011, No 4, pp. 322-331.
17. R i a d, A. M., A. H. H u s s e i n, H. M. K a s e m, A. A. E l-A z m. A New Efficient Image Encryption Technique Based on Arnold and IDEA Algorithms. – ICIIP, Vol. **46**, 2012, pp. 140-145.
18. S i n g h, H. P., S. V e r m a, S. M i s h r. Secure-International Data Encryption Algorithm. – International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. **2**, 2013, No 2, pp. 780-792.
19. W o r t h i n g t o n, B. An Introduction to Hill Ciphers Using Linear Algebra. University of North Texas, 2010, pp 1-24.
20. B i b h u d e n d r a, A., S. K. P a n i g r a h y, S. K. P a t r a, G. P a n d a. Image Encryption Using Advanced Hill Cipher Algorithm. – IJRTER, Vol. **1**, 2009, No 1 pp. 663-667.
21. M i s h r a, D. C., R. K. S h a r m a. Grayscale-Image Encryption Using Random Hill Cipher over $SL_n(F)$ Associated with Discrete Wavelet Transformation. – AAM: An International Journal, Vol. **8**, 2013, No 2, pp. 777-791.
22. Y a n g, C., M. H u a, S. J i a. Image Encryption Algorithm Based on Chaotic Mapping and Chinese Remainder Theorem. – Metallurgical and Mining Industry, 2015, No 4, pp. 206-212.
23. K o n g, L., L. L i. A New Image Encryption Algorithm Based on Chaos. – In: Proc. of 35th Chinese Control Conference, IEEE, 2016, pp. 4932-4937.
24. C h e n, T., M. Z h a n g, J. W u, C. Y u e n, Y. T o n g. Image Encryption and Compression Based on Kronecker Compressed Sensing and Elementary Cellular Automata Scrambling. – Optics & Laser Technology, Elsevier, Vol. **84**, 2016, pp. 118-133.
25. H u a, Z., Y. Z h o u. Image Encryption Using 2D Logistic-Adjusted-Sine Map. – Information Sciences, Elsevier, Vol. **339**, 2016, pp. 237-253.

26. T a n g, Z., J. S o n g, X. Z h a n g, R. S u n. Multiple-Image Encryption with Bit-Plane Decomposition and Chaotic Maps. – Optics and Lasers in Engineering, Elsevier, Vol. **80**, 2016, pp. 1-11.
27. Y e, G. Image Scrambling Encryption Algorithm of Pixel Bit Based on Chaos Map. – Pattern Recognition Letters, Elsevier, Vol. **31**, 2010, pp. 347-354.
28. A b d u l, N., M. A b b a s. Image Encryption Based on Independent Component Analysis and Arnold's Cat Map. – Egyptian Informatics Journal, Elsevier, Vol. **17**, 2015, pp. 139-146.
29. L i n, Z.-H., H.-X. W a n g. Image Encryption Based on Chaos with PWL Memristor in Chua's Circuit. – ICCCAS, IEEE, 2009, pp. 964-968.
30. Z h a n g, H., R. C a i. Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic Systems Combination. – ICISS, IEEE, 2010, pp. 113-117.
31. T a n g, Z., X. Z h a n g, W. L a n. Efficient Image Encryption with Block Shuffling and Chaotic Map. – Multimed Tools Appl., Springer, Vol. **74**, 2014, No 15, pp. 5429-5448.
32. Z h a n g, Y. P., P. X u, L. Z. X i a n g. Research of Image Encryption Algorithm Based on Chaotic Magic Square. – Advances in ECWAC, Springer, Vol. **2**, 2012, pp. 103-109.
33. W a n g, D., C.-C. C h a n g, Y. L i u, G. S o n g, Y. L i u. Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values. – International Journal of Network Security, Vol. **17**, 2015, No 3, pp. 322-327.
34. M i l a n o v, E. The RSA Algorithm. 3 June 2009. **https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf**
35. V i n o t h i n i, S a r a n y a, V a s u m a t h i. A Study on RSA Algorithm for Cryptography. – IJCSIT, Vol. **5**, 2014, pp. 5708-5709.
36. A n a n d a k u m a r, S. Image Cryptography Using RSA Algorithm in Network Security. – IJCSET, Vol. **5**, 2015, No 9, pp. 326-330.
37. C h a n d e l, G. S., P. P a t e l. A Review: Image Encryption with RSA and RGB Randomized Histograms. – IJARCCE, Vol. **2**, 2013, No 11, pp. 4391-4401.
38. O s w a l d, E. Introduction to Elliptic Curve Cryptography. 2005. **http://www.vanilla47.com/PDFs/Cryptography/Miscellenea/Introduction_to_Elliptic_Curve_Cryptography.pdf**
39. M o h a m e d, A., S. E l d e e n, A b d e l l a t i f, A. E l k o u n y, S. E l r a m l y. DES Algorithm Security Fortification Using Elliptic Curve Cryptography. – ICCES, IEEE, 2015, pp. 335-340.
40. S u g a n y a, N., S. S a t h i y a. Encryption of Image Matrix Using Elliptic Curve Cryptography. – IJITE, Vol. **2**, 2012, pp. 229-232.
41. S h u a n g y u a n, Y., L. Z h e n g d i n g, H. S h u i h u a. An Asymmetric Image Encryption Based on Matrix Transformation. – ISCIT, IEEE, Vol. **1**, 2004, pp. 66-69.
42. K e s t e r, Q.-A., L. N a n a, A. C. P a s e u. A New Hybrid Asymmetric Key-Exchange and Visual Cryptographic Algorithm for Securing Digital Images. – In: Proc. of International Conference on AST, IEEE, 2013, pp. 1-5.
43. S a s i, S., D. L. S w a r n a J y o t h i. A Heuristic Approach for Secured Transmission of Image Based on Bernstein Polynomial. – In: Proc. of International Conference on Circuits, Communication, Control and Computing, IEEE, 2013, pp. 312-315.
44. C h h o t a r a y, S. K., A. C h h o t a r a y, G. S a n k a r R a t h. A New Method of Generating Public Key Matrix and Using It for Image Encryption. – In: Proc. of 2nd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, 2015, pp. 453-458.
45. E l a s h r y, I., O. A l l a h, A. A b b a s, S. E l-R a b a i e, F. E l-S a m i e. Homomorphic Image Encryption. – Journal of Electronic Imaging, Vol. **18**, 2009, No 3, pp. 1-14.
46. E l-F i s h a w y, N., O. Z a i d. Quality of Encryption Measurement of Bitmap Images with Rc6, Mrc6, and Rijndael Block Cipher Algorithms. – International Journal of Network Security, Vol. **5**, 2007, No. 3, pp. 241-251.
47. K a m a l i, S., R. S h a k e r i a n, M. H e d a y a t i, M. R a h m a n i. A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. – In: Proc. of International Conference on Electronics and Information Engineering, IEEE, Vol. **1**, 2010, pp. 1-141.
48. A h m a d, J., F. A h m e d. Efficiency Analysis and Security Evaluation of Image Encryption Schemes. – International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, Vol. **12**, 2012, No 4, pp. 18-31.

49. S h a n n o n, C. Communication Theory of Secrecy Systems. – Bell System Technical Journal, Vol. **28**, 1949, No 4, pp. 656-715.
50. L i a n, S. Multimedia Content Encryption: Techniques and Applications. Auerbach Publications, CRC Press, Taylor and Francis Group. 2008.
51. E l k a m c h o u c h i, H., M. M a k a r. Measuring Encryption Quality for Bitmap Images Encrypted with Rijndael and Kamkar Block Ciphers. – In: Proc. of 22nd IEEE National, Radio Science Conference (NRSC'05), 2005, pp. 277-284.
52. A h m e d, H., H. K a l a s h, O. A l l a h. Encryption Efficiency Analysis and Security Evaluation of Rc6 Block Cipher for Digital Images. – In: Proc. of International Conference on Electrical Engineering, IEEE, 2007, pp. 1-7.
53. E l-l s k a n d a r a n i, M., S. D a r w i s h, S. A b u g u b a. A Robust and Secure Scheme for Image Transmission over Wireless Channels. – In: Proc. of 42nd Annual International Conference on CST, IEEE, 2008, pp. 51-55.
54. R a n j a n, K. H. S., H. R. P. K u m a r, K. B. S u d e e p a, G. A i t h a l. Enhanced Security System Using Visual Cryptograhy and Symmetric Encryption. – International Journal of Advances in Engineering & Technology (IJAET), Vol. **6**, 2013, No 3, pp. 1211-1219.
55. N a o r, M., A. S h a m i r. Visual Cryptography. – Proceedings of Advances in Cryptology, EUROCRYPT 94, Springer-Verlag, LNCS, Vol. **950**, 1994, pp. 1-12.
56. P r a b i r, K. N a s k a r, A y a n C h a u d h u r i, D e b a r a t i B a s u, A t a l C h a u d h u r i. A Novel Image Secret Sharing Scheme. – In: Proc. of 2nd International Conference on Emerging Applications of Information Technology, IEEE, 2011, pp. 177-180.
57. S h a r m a, H., N. K u m a r, G. K. J h a. Enhancement of Security in Visual Cryptography System Using Cover Image Share Embedded Security Algorithm (CISEA). – In: Proc. of International Conference on Computer & Communication Technology (ICCCT'11), IEEE, 2011, pp. 462-467.
58. K a f r i, O., E. K e r e n. Encryption of Pictures and Shapes by Random Grids. – Optics Letters, Vol. **12**, 1987, pp. 377-379.
59. H a w k e s, L. W., A. Y a s i n s a c, C. C l i n e. An Application of Visual Cryptography to Financial Documents. Technical Report, Florida State University, 2000.
60. L i, M.-J., J. S.-T. J u a n. A Flexible Multiple-Secret Image Sharing Scheme by Shifting Random Grids. – In: Proc. of 17th International Symposium on Consumer Electronics (ISCE'13), IEEE, 2013, pp. 289-290.
61. J o y, J., Y. C h a n g, S. J u s t i c e, T. J u a n. Multi VSS Scheme by Shifting Random Grids. – World Academy of Science, Engineering and Technology, Vol. **67**, 2012, pp. 936-942.
62. J o t h i, R., A. O j h a. On Multi-Secret Sharing Using Hill Cipher and Random Grids. – In: Proc. of International Conference on Advances in Computer Engineering and Applications (ICACEA'15), IEEE, 2015, pp. 683-687.
63. C h e n, W.-K. Image Sharing Method for Gray-Level Images. – Journal of Systems and Software, Vol. **86**, 2013, pp. 581-585.
64. S r u t h y, K., J. R. R a m e s h. Random Grid Based Visual Cryptography Using a Common Share. – In: Proc. of International Conference on Computing and Network Communications (CoCoNet'15), IEEE, 2015, pp. 656-662.
65. L i u, F., C. W u. Embedded Extended Visual Cryptography Schemes. – IEEE Transactions on Information Forensics and Security, Vol. **6**, 2011, No 2, pp. 307-322.
66. A s k a r i, N., H. M. H e y s, C. R. M o l o n e y. An Extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images. – In: Proc. of 26th Annual IEEE Canadian Conference on Electrical and Computer Engineering, 2013, pp. 1-6.
67. K a n g, I., R. G o n z a l o, A r c e, H.-K. L e e. Color Extended Visual Cryptography Using Error Diffusion. – ICASSP, IEEE, 2009, pp. 1473-1476.