A Review on Various Digital Image Encryption Techniques and Security Criteria

Mohit Kumar
Research scholar
Amity University Haryana
India

Akshat Aggarwal
Assistant Professor
Amity University Haryana
India

Ankit Garg
Assistant Professor
Amity University Haryana
India

ABSTRACT
Images excessively contribute to communication in this era of multimedia. When a user transfers images over an unsecured communication network, then the absolute protection is a challenging issue to conserve the confidentiality of images. Encryption is a method of retaining the secrecy of images. This paper provides the succinct introduction to the cryptography, moreover, includes a concise description of various elemental securities' criteria of the image encryption algorithms. This work presents the survey of diverse image encryption techniques and comparison of discrete image encoding approaches, at last discloses a conclusion and suggests future works.

General Terms
Image security, image encryption, image processing.

Keywords
Encrypted image; histogram; image, image encryption; image security parameters; permutation and substitution; scrambling, XOR operation.

1. INTRODUCTION
The Internet and information technology are sprouting swiftly. As a result, people are widely using interactive media in communication. For instance; image, audio, and video. Images occupy the copious fraction of multimedia. Images play a significant role in communication, for example; military, national-security agencies and diplomatic affairs. Since, these images may carry highly confidential information, so these images entail extreme protection when users amass somewhere over an unreliable repository. Furthermore, when people wish to transfer images over an insecure network, then it becomes crucial to provide an absolute protection. In brief, an image requires protection against various security attacks.

The primary intention of keeping images protected is to maintain confidentiality, integrity and authenticity [16]. Different techniques are available for making images secure and one technique is encryption. Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image [16], which is usually a reverse execution of the encryption process. For illustration, Figure 1 represents a primary image; a user operates an encryption technique and produces a secrete image; Figure 2 shows an encrypted image that is the output of an encoding process. On the other hand, when a receiver gets this hidden image, he applies the decryption process and recovers the original information. Figure 3 illustrates the recovered image.

Fig 1: Panda

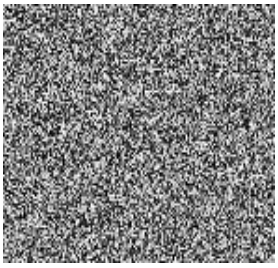

Fig 2: Cipher

Fig 3: Recovered image (Panda)

Primarily, cryptography has two main categories; (1) symmetric key cryptography, (2) asymmetric key cryptography [16].

In symmetric or secret key cryptography, senders and recipients use a same key in encryption and decryption [16].

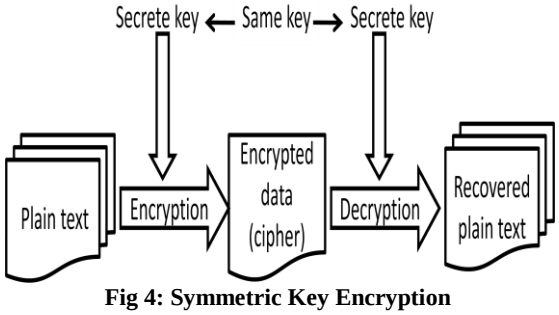

Fig 4: Symmetric Key Encryption

Asymmetric or public key cryptography uses different keys in encrypting and decrypting messages [16]. This technique applies a public key and a private key to encode and decode an image respectively. However, both keys are unique, but mathematically have a connection.

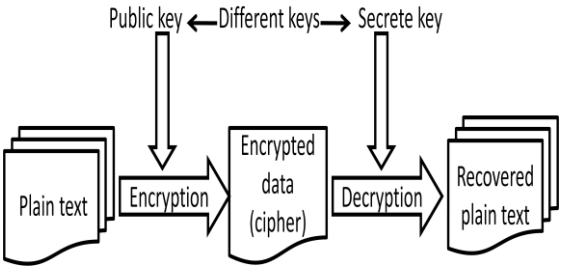

Fig 5: Asymmetric Key Encryption

In addition, hashing authenticates the received image due to having the one way property.

The diverse algorithms are accessible to encrypt information, specifically; RSA, DES, AES, etc. However, these algorithms are paramount to encipher a text data, nevertheless, inept for the image encryption [6]. Since, images have intrinsic features such as abundant redundancy and a strong correlation between adjoining pixels [6]. So, one can easily infer the value of neighbors of a pixel. Hence, images need an efficient method to achieve an invulnerable security.

Primarily, image encryption techniques rely on three methods; (1) pixel permutation: the algorithm scrambles the pixels [22, 23], (2) pixel substitution: the encryption method modifies the pixel value [22, 23], (3) visual transformation [22, 23].

Furthermore, the artificial neural network (ANN) is a different approach to protect an image and helpful due to its nonlinear and one way properties [11]. In ANN, to calculate the final result is easy, in contrast, retrieving raw data from the outcome is a problematic task. Thus, it will be unfeasible to decide initial data from the result back devoid of weights and bias [11]. Figure 6 is a feed forward neural network, and formula (1) helps figure out the output of the network.

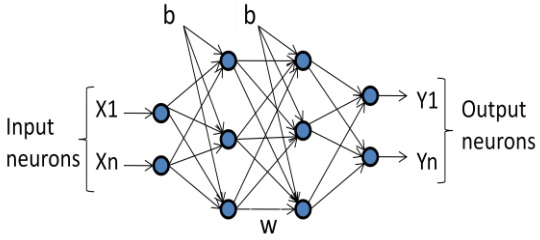

Fig 6: Artificial Neural Network

$$Y = f(\sum_{i=1}^{n} W_i X_i + b) \qquad (1)$$

Where *Y* is output, *W* is the weight, *X* is an input; *b* is bias and n is the number of neurons in different layer.

Furthermore, compression is another technique to encode an image through abbreviating an image. Therefore, the compressed form of an image is difficult to understand. In addition, the main advantage of encryption through a compression process is that it reduces the size of an image without losing the information provided that lossless compression. However, lossy compression can be used where a slight distortion is acceptable.

2. INTRODUCTION TO IMAGE SECURITY PARAMETERS

Generally, an excellent encryption technique qualifies various security criteria and some of them are following as:

2.1 Large key space: An enormous key space is necessary to thwart the brute force attack [2]. For example, the key of size 512 bits provides the key space of 2^{512} ($\cong 10^{154}$ possible combinations). Thus, if a computer does 10^{10} calculations per second, will take about 10^{136} years to find the right key.

2.2 Key sensitivity: It ensures that the system will generate completely contrary consequence, despite a whit change in key [8]. Thus, an encryption technique should be key sensitive.

2.3 Uniform Image histogram: Histogram provides information about the frequency distribution of continuous pixels and density estimation [19, 20]. So a cipher image should have a uniform histogram to be secure from the known plain-text attack [21]. For example, figure 7 is the histogram of the original image and figure 8 is the histogram of the encrypted image. Figure 8 shows the more uniform histogram that is highly desirable.

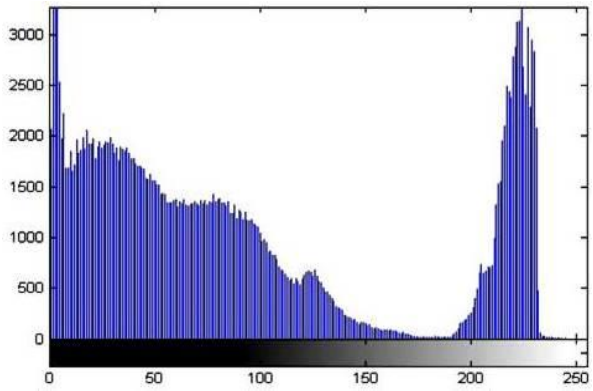

Fig 7: Histogram of an original image

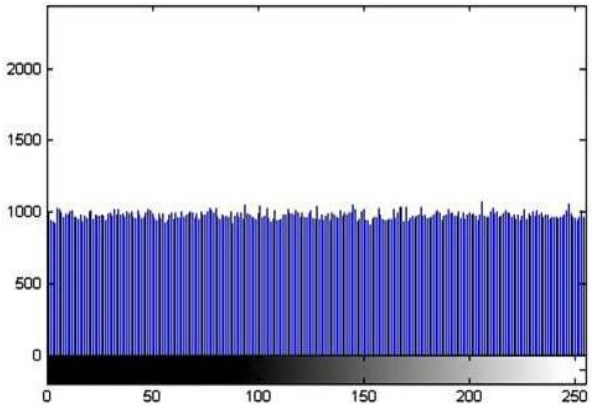

Fig 8: Histogram of Cipher Image

2.4 Information entropy: It identifies the degree of uncertainty and uniform distribution in the system [17]. Thus, an encryption technique should show randomness and uniform distribution in the encryption process. Information entropy is calculated by the following formula (2).

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i) \log_2 \left[P(m_i)\right] \qquad (2)$$

Where p (m_i) defines the probability of a pixel and N is the number of bits in each pixel. For a gray level image, each pixel has 8 bits, so the probability of a pixel is $1/2^8$. Hence, information entropy of the gray level image is H (m) = 8. However, practically it is intricate to obtain ideal entropy; so slight difference is also tolerable.

2.5 Correlation analyses: It assesses the correlation between two adjoining pixels of the plain-image and the cipher image [17]. An encrypted image should have low correlation between two abutting pixels. For example, x_i and y_i are two pixel pair then the correlation coefficient can be calculated by equation (6) [24].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \ , \qquad (3)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \qquad (4)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\,(y_i - E(y)) \ , \qquad (5)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \ , \qquad (6)$$

where $\sqrt{D(x)} \neq 0$ and $\sqrt{D(y)} \neq 0$

Where x_i and y_i are gray level value of two adjacent pixels, N is the number of pairs (x_i, y_i) and E(x) is the mean of xi and E(y) is the mean of y_i.

2.6 Differential analyses: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) measures the invulnerability of an algorithm against the differential attacks on image [17]. NPCR evaluates the pixels change rate in the coded image after modification in one pixel of a prime image [17] [18], consequently, high NPCR value is effective. Furthermore, UACI computes the variation in intensity of the corresponding pixel of the plain-image and the encrypted image [18]. If C1 and C2 are the two cipher image after and prior to 1 bit change in the original image, then NPCR and UACI can be calculated by following formula (7) and (8) respectively [24].

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \ \times 100\ \% \ , \qquad (7)$$

With if C1 (i, j) = C2 (i, j), then D (i, j) = 0 else D (i, j) = 1,

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\ \%}{M \times N}, \qquad (8)$$

Where, M and N are the dimension and (i, j) is the coordinates of the image.

3. IMAGE ENCRYPTION TECHNIQUES

3.1 Image Encryption Using Affine Transform and XOR Operation (2011)

In this assignment, Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [1] have imparted a technique, which applies 64 bits key in the encryption. Firstly, the designed technique operates the affine transformation to dispel the pixels by applying four sub keys of 8 bits. Thereafter, the algorithm decomposes an image into 2*2 pixel block size, and afterward, applies a XOR operation on each block with four sub key of 8 bits to modify pixels value. Figure 9 illustrates an original image. The imparted system operates the transformation operation on the original image to produce a transformed image. Afterward, proposed technique applies the XOR operation on this transformed image to produce a complete cipher image Figure 9 illustrate the original; figure 10 denotes the transformed image and figure 11 represents the coded image. Figure 12 and 13 shows histogram of the original and the encrypted image respectively.

Fig 9: Car

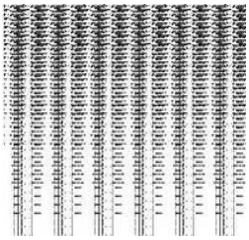

Fig 10: Transformation operation

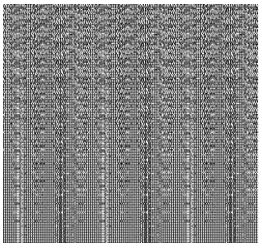

Fig 11: Cipher image after XOR operation

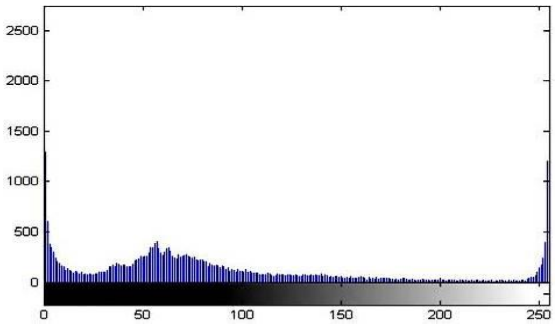

Fig 12: Histogram of the original car

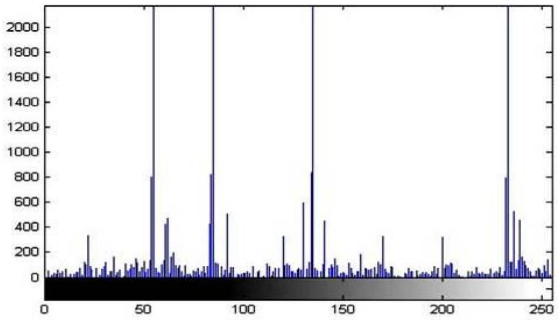

Fig 13: Histogram of Cipher

The consequences disclose that the presented method is less effective in reducing the correlation between pixels and also has short key space. This algorithm does not have adequate complexity in procedure of key used by the encryption process. So, imparted technique does not provide the feasible security level to images due to short key and simple XOR operation.

3.2 A New Chaotic System for Image Encryption (2012)

In this script, Long Bao and Yicong Zhou have [2] suggested a new chaotic system that constitutes the three distinct one-dimensional chaotic maps. The suggested technique applies the Logistic map as a controller to choose the Tent map or a

Sine map to generate random sequences [2]. Thereafter, the imparted algorithm utilizes the substitution-permutation network (SPN) structure to obtain the confusion and diffusion property [2, 15]. This scheme uses 240 bit key for large key space. Mainly, this key contains all parameter settings and the initial values of the new chaotic system, and excessive sensitivity in key changes for encryption and decryption. Consequently, the proposed approach provides an excellent security against the brute force attack as well as extreme key sensitivity and chaotic behavior.

3.3 A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling (2012)

In this treatise, Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue [3] have propounded a one-dimensional random scrambling based technique. At the beginning, the algorithm transforms a two-dimensional image into the one-dimensional vector and then applies the one-dimensional random shuffling [3]. Thereafter, the method performs an anti transformation on the dispersed vector to generate an encipher image. Consequently, the imparted scheme does not require the iterative computation, since, one or two executions are sufficient for the best effect. Figure 14 shows an original image; after operating the first iteration of the procedure, technique produces an encoded image, which is illustrated in figure 15. After operating 15 rounds; a usable cipher image is produced, which is represented in figure 16. Moreover, figure 17 and figure 18 shows the histogram of the original image (dog) and the cipher image respectively.

Fig 14: Dog

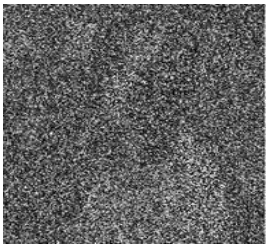

Fig 15: Cipher at iteration 1

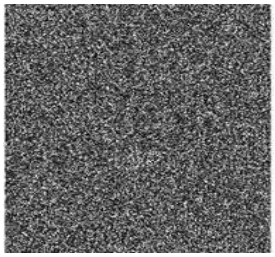

Fig 16: Cipher at iteration 15

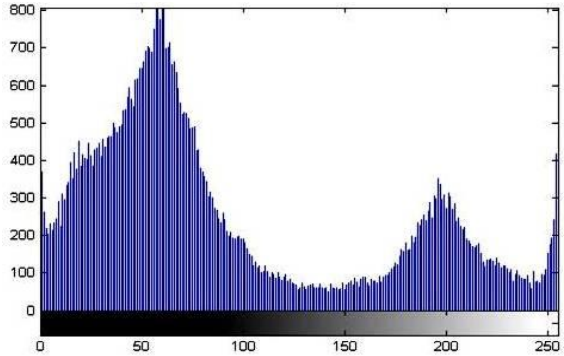

Fig 17: Histogram of dog image

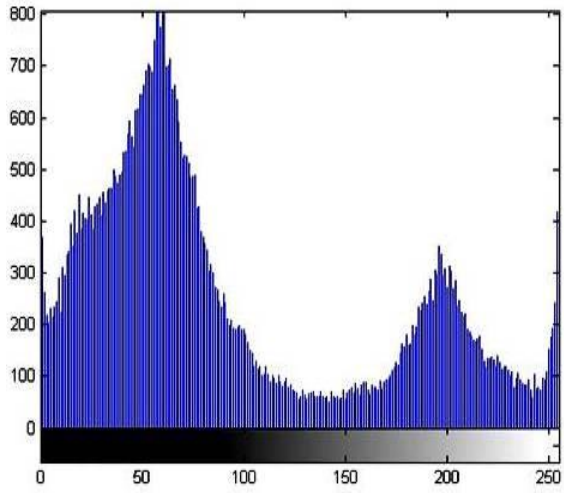

Fig 18: Histogram of the cipher image

After experimenting, it is observed that the histogram of the original image and the cipher image is same due to only scrambling process. However, the scrambling process decreases the correlation between pixels, but has no impact on the histogram. Since, the histogram of the cipher image will reveal ample information about the original image. So, suggested technique is less suitable for highly confidential images.

3.4 A Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel (2012)

In this paper, Amnesh Goel and Nidhi Chandra [4] have put forward an effective system which decomposes the original image into n*n block size. Afterward, the technique uses a transformation algorithm to minimize the correlation between pixels [4]. Mainly, the imparted technique consists of two main stages. At the first stage, the algorithm performs horizontal block displacement followed by the vertical block displacement. Thereafter, in the second stage, the technique performs inter pixel displacement of RGB values. Each stage has its own stage mask or key, which is utilized in the process [4]. Figure 19 represents an original image of size 300*300 and after applying horizontal block displacement on this image, figure 20 is generated. Furthermore, after operating vertical block displacement on the horizontally displaced image, an image is produced that is illustrated in figure 21. Afterward, applying inter pixel displacement in RGB values, a cipher image is produced, which is presented in figure 22.

Fig 19: Original Image

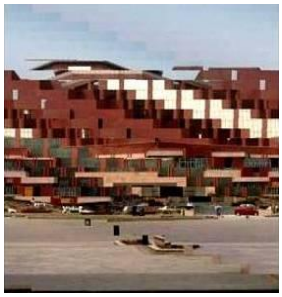

Fig 20: Horizontal displacements at (10*10) block size

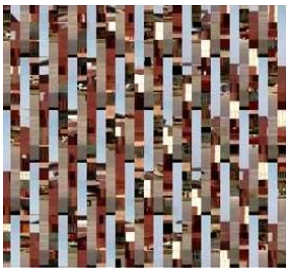

Fig 21: Vertical displacements at 10*10 blocks size

Fig 22: Cipher Image

The experimental outcomes validate that the propounded system generates a robust cipher image with the help of explosive displacement in RGB values.

3.5 A Novel Neural Network Approach for Digital Data Encryption/Decryption (2012)

In this treatise, Saraswati D. Joshi, Dr. V.R. Udupi and Dr. D.R. Joshi [5] have put forth a technique, which scans an image pixel by pixel. Afterward, it carries out the transformation on these pixels using substitution and permutation. Furthermore, the encoding procedure inserts the impurity in the transformed image to garble. This system uses two levels of enciphering to achieve potent security. Moreover, the imparted scheme employs an Artificial Neural Network to decrypt the cipher image. Decryption involves three stages [5]. At the first stage, the system eliminates the added impurity. Afterward, in the second stage, network discards the extra conjoined columns in the matrix. In addition, in the third stage, received image data and weights which were stored after training, are utilized to stimulate the network. The dominance of this method is due to avail random encryption on the sender side and averts the prerequisite key exchange. Therefore, proposed technique provides a potent safety level. The disadvantage is that decryption process is more time consuming.

3.6 A Novel Encryption method for Image Security (2012)

In this paper, Mohammed Abbas and Fadhil Al-Husainy [6] have contrived an approach that relies on the bit level permutation. In general, this system utilizes two Boolean operations: XOR and Rotation on the bits of the pixels to satisfy the confusion and diffusion properties. Furthermore, to encrypt an image, the algorithm applies a sequential XOR function on all bits of pixels in the image followed by the circular right rotation of these bits. Thereafter, the technique repeats these two activities multiple times to ensure better security. Moreover, this method uses a common secret key for encryption and decryption. Figure: 23 is a primary image, and the figure 24 is encrypted image, which is completely dissimilar from the original image.

Fig 23: Original Image

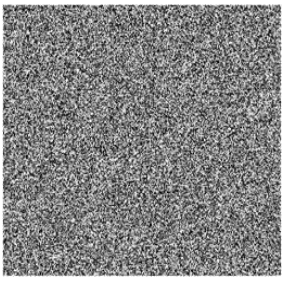

Fig 24: Cipher Image

3.7 A Two Layer Chaotic Network Based Image Encryption Technique (2012)

In this paper, Anchal Jain and Navin Rajpal [7] have imparted a technique that relies on the diffusion and substitution. The proposed system applies two-layer chaotic neural networks in the encryption and decryption. Furthermore, this approach utilizes a logistic chaotic map; to design weights and biases for the neural network, and an external key that provides the initial condition [7]. Generally, the propounded algorithm applies the key of 80 bits. However, the generation of chaotic sequence is same in the encoding and decoding [7]. The method uses the first layer of the network for the diffusion and the second layer for the substitution, while in the decipherment; the arrangement of layers is in reverse order. Consequently, the provided technique provides significant security against the brute force attack and the known plaintext or chosen plaintext attack.

3.8 A New Cryptographic Approach for Image Encryption (2012)

In this script, Nidhi Sethi and Dipika Sharma [8] have provided an encryption technique, which takes advantage of logistic mapping to encipher and compress an image. The complete execution of the proposed algorithm is following as; at first, the imparted scheme abbreviates an image through Haar Wavelet transformation. Afterward, the system decomposes the figure into 8*8 size of the block; and then this dismembered picture goes into the coding process. Generally, this encoding procedure has two stages. At first, the propounded program minimizes the inter pixel correlation by using a block based scrambling. This shuffling method utilizes a crossover approach that relies on genetic algorithm [8]. Furthermore, in the second stage, the system uses a 2D Logistic map to encrypt pixel values of the dispelled facsimile. Moreover, the Logistic based mode satisfies the confusion and diffusion properties in the cipher picture. Thereafter, the logistic map generates the key that is sent to the receiver by watermarking method for potent security. Results show that the suggested strategy can offer feasible protection.

3.9 SD-AEI: An Advanced Encryption Technique for images (2012)

In this paper, Somdip Dey [9] has imparted a combined technique. Basically, the propounded approach depends on the three methods of cryptography: (1) Bits rotation and reversal, (2) Extended Hill Cipher, (3) Modified MSA Randomization [9]. Furthermore, the proposed system utilizes four stages to encrypt an image. At first stage, the algorithm generates a unique number from the symmetric key. In the second stage, bit's rotation and reversal are done, based on the length of a symmetric key. Afterward, in the third stage, the system applies Extended Hill Cipher technique for the encryption. Thereafter, in the fourth stage, the scheme uses the modified MSA randomization approach for substitution. The empirical results corroborate that SD-AEI encoding procedure is dominant on the SD-EI due to additional randomization.

3.10 Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location (2012)

In this treatise, Hazern Mohammad Al-Najjar [10] has offered an overture of an image encryption technique which is based on the multidimensional chaotic function. This system dispels the pixels and alters the value of pixels. The imparted

approach changes the pixel value by applying the two substitution methods and uses the two scrambling processes to scatter the pixels. Furthermore, the suggested course encrypts an image as follows: the algorithm applies the first substitution scheme using the column index value, followed by the first scrambling method which utilizes the X, Y, Z planes of Rossler equation [10]. Afterward, the system operates the second replacement procedure using row index followed by the second shuffling plan which employs X, Y, Z planes [10]. The observations corroborate that this algorithm is sensitive to the initial condition and also invulnerable to a brute force attack and other types of attacks due to large key space that is 10^45.

3.11 Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP (2012)

In this exposition, Dattatherya, S. Venkata Chalam and Manoj Kumar Singh [11] have propounded an image encryption technique that comprises three tasks: compression, security and the authentication. The proposed method uses an artificial neural network to accomplish these tasks. The offered scheme uses the universal approximation for the compression. In addition, the imparted approach applies the feed forward neural network for compression; in which, the hidden layer has the least number of neurons compared to the input layer. The advised procedure assures the security due to the one way property of neural networks. Furthermore, the system provides the authenticity by the one to one mapping. The aftereffects validate that this method provides adequate safety along with the feature of detecting the tampered area of an image. Separate parts of the system are illustrated in the figures given below. Figure 25 shows the architecture of an artificial neural network, which is trained for the compression. Figure 26 represents a compression module, which is used for the abridgement and generates a compact output for a block. Moreover, Figure 27 displays a module, which decompresses the squashed data for a block.

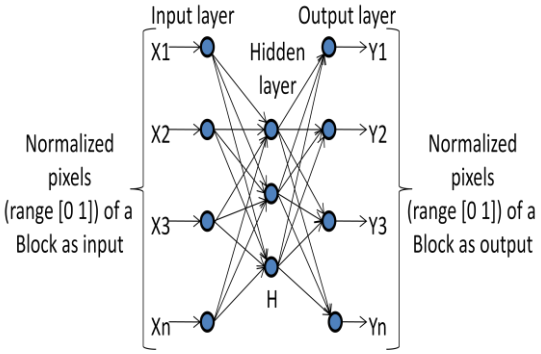

Fig 25: Architecture of Artificial Neural Network for compression training

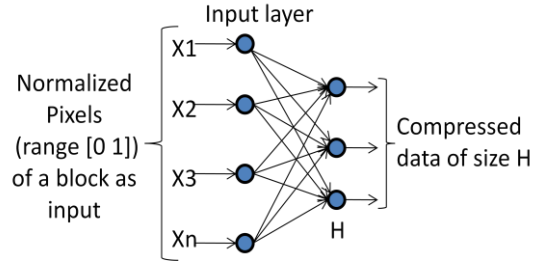

Fig 26: Compression part of Artificial Neural Network

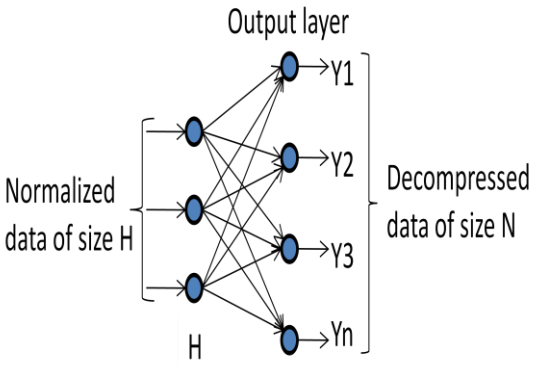

Fig 27: Decompression part of Artificial Neural Network

3.12 Image Encryption and Decryption Using Blowfish Algorithm in MATLAB (2013)

In this treatise, Pia Singh and Karamjeet Singh [12] have connoted a technique which is based on the blowfish algorithm. Generally, the Blowfish algorithm is the 64-bit symmetric block cipher that repeats simple function 16 times and applies a variable key length range from 32 to 448 bits [12]. The offered system follows the two processes; the first is a key expansion, and the second is a data encryption. Furthermore, the Blowfish algorithm includes two exclusive-or operations that are performed after 16 rounds and a swap operation. The aftermaths corroborate that blowfish technique is fast and secure.

3.13 Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map (2013)

In this script, Riah Ukur Ginting and Rocky Yefrences Dillak have [13] propounded an algorithm which relies on the RC4 Stream Cipher and Chaotic Logistic map. The proposed technique consists of three stages. In the first stage, system converts the external key into the initial value. Afterward, in the second stage, the technique applies the initial value to the Chaotic Logistic Map for engendering a pseudo random number. Afterward, in the third stage, the system XOR the byte stream of the plain image with the stream of pseudo random number for the encryption. Experimental outcomes of this encryption algorithm validate that the decryption process is the highly key sensitive.

3.14 GS-IES: An Advanced Image Encryption Scheme (2013)

In this article, Gurpreet Singh and Amandeep Kaur [14] have propounded an advance version of the SD-IES technique by adding a new permutation block in the SD-IES technique. The propounded algorithm has five stages. In the first stage, the technique uses the RSA algorithm to generate a password and perform the one-bit rotation based on the generated password. Moreover, in the second stage, the suggested technique applies the extended hill cipher technique to form encryption invulnerable. Furthermore, in the third stage, the technique performs the bit's reversal. Afterward, in the fourth stage, the system performs a permutation and combination rotation using password length and in the fifth stage, the encrypted image is stored. The observations corroborate that the GS-IES algorithm is dominant on the previous SD-IES due to the inclusion of permutation block in the last stage.

4. COMPARION OF VARIOUS IMAGE ENCRYPTION TECHNIQUES

Comparison is done on the basis of; key space, key sensitivity, entropy of original and cipher image, and change in the histogram after encryption, correlation coefficient of original image and cipher image and NPCR values.

Table 1: Comparison of various image encryption algorithms

S. N	Authors	Technique Used	Key space	Key sensitivity	Entropy		Histogram	Correlation		NPCR %
					Original	*Cipher*		*Original*	*Cipher*	
1	A. Nag, J.P. Singh, S. Khan, S. Biswas et.al [1]	Transformation & XOR	2^{64}	Low	6.0729	7.0513	Not good	.3232	.0381	0 (negligible)
2	Long Bao and Yicong Zhou [2]	Three one-dimensional chaotic map	2^{240}	Very high	7.5528	7.9662	Good	.9212	.0031	99.61
3	Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue [3]	One dimensional random scrambling	Not fix	High	7.6330	7.6330	No change (same as original image)	.1915	.0059	99.36
4	Mohammed Abbas and Fadhil Al-Husainy [6]	Bit level permutation, XOR & rotation	Not fix	High	7.7502	7.9967	Good	.5605	.0041	0 (negligible)
5	Nidhi Sethi and Deepika Sharma [8]	Two dimensional logistic map & compression	10^{112}	High	7.6573	7.9895	Good	.9368	.0182	0 (negligible)
6	Hazern Mohammad Al-Najjar [10]	Multi-dimension chaotic function	10^{45}	High	7.5672	7.997	Good	.9462	.01542	99.63

The zero or negligible NPCR value means that the technique achieves negligible NPCR (less than .01%).

5. CONCLUSION

This work has a survey of distinct image encryption algorithms, and concludes that the chaotic approach exhibits extreme uncertainty and provides incredible safety. Moreover, study discloses that NPCR does not depend on the key sensitivity; so, to achieve satisfactory NPCR in the block based encryption methods, the values of an encrypted block should be dependent on the other cipher blocks. Furthermore, results show that scrambling alone is not sufficient to offer the remarkable security; there should be a substitution along with shuffling. Consequently, this review infers that a preeminent image encoding technique has the following characteristics to provide extraordinary protection; (1) Provide large key space, (2) Highly key sensitive, (3) Generate a uniform histogram, (4) Satisfy to Shannon's confusion and diffusion property, (5) Reduce correlation effectively between two adjacent pixels, (6) Provide uncertainty in the system, (7) High NPCR value (near to 100%) and suitable UACI rate (near to 33 %). Moreover, besides these given attributes, an encryption technique should be fast enough to encipher an image.

At last, a conclusion is that all examined encryption algorithms in this paper, are effective and have their own merits and demerits in respect of speed and security trade off.

6. FUTURE WORK

Since, the calculation capabilities of machines are rapidly thriving, and the majority of the image encryption techniques have several deficiencies in terms of speed and safety adjustment. Consequently, image enciphering algorithms demand a continuous, efficient enrichment. Furthermore, the images occupy more space compared to text data and require more bandwidth to be transferred over the network. Predominantly, there is a dearth of outstanding image encryption methods that can also reduce the size (compress image) of the encoded image. In addition, a receiver demands that the decrypted image should produce the original

information without any distortion. So now necessity requires working in space, speed and security trade off.

7. ACKNOWLDGEMENT

Author is thankful to his guides Mr. Akshat Agrawal and Mr. Ankit Garg who give him an opportunity to carry out this work. Author is also thankful to NPTEL which provides E-learning through online Web and Video courses in Engineering, Science and humanities streams.

8. REFERENCES

[1] Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar "Image Encryption Using Affine Transform and XOR Operation" 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[2] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73 .

[3] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669-1672.

[4] Amnesh Goel, Nidhi Chandra "A Technique for Image Encryption Based On Explosive n*n Block displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel" 2012 International Conference on Communication Systems and Network Technologies, 11-13 May 2012, page: 884-888.

[5] Saraswati D. Joshi, Dr. V.R. Udupi, Dr. D.R. Joshi, "A Novel Neural Network Approach for Digital Image Data Encryption/Decryption", Power, Signals, Controls and Computation (EPSCICON), 2012 International Conference on 3-6 Jan. 2012, pages: 1-4.

[6] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", International Journal of Security and Its Applications, vol.6, no.1, January 2012, pages: 1-8.

[7] Anchal Jain, Navin Rajpal, "A Two Layer Chaotic Network Based Image Encryption Technique", Computing and Communication Systems (NCCCS), 2012 National Conference on 21-22 Nov.2012, pages: 1-5.

[8] Nidhi Sethi, Deepika Sharma, "A New Cryptographic Approach for Image Encryption", Parallel, Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on 6-8 Dec. 2012, pages: 905-908.

[9] Somdip Dey, "SD-AEI: An Advanced Encryption Technique for Images", Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on 10-12 July 2012, pages: 68-73.

[10] Hazem Mohammad Al-Najjar, "Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012, pages: 354-357.

[11] Dattatherya, S. Venkata Chalam & Manoj Kumar Singh, "Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP", International Journal of Image Processing (IJIP), Volume (6), Issue (1), 25 Feb 2012, pages: 13-25.

[12] Pia Singh, Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013, pages: 150-154.

[13] Riah Ukur Ginting, Rocky Yefrences Dillak, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Technology and Electrical Engineering (ICITEE), 2013 International Conference on 7-8 Oct. 2013, pages: 101-105.

[14] Gurpreet Singh, Amandeep Kaur, "GS-IES: An Advanced Image Encryption Scheme" International Journal of Engineering Research & Technology, Vol. 2 Issue 9, September – 2013, pages: 465-468.

[15] D. R.Stinson, Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006.

[16] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.

[17] Shujiang Xu, Yinglong Wang, Jizhi Wang, Yucui Guo, "A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map", 2010 2nd International Conference on Signal Processing Systems (ICSPS), 5-7 July 2010, pages: v2-326-v2-330.

[18] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", Chaos, Solitons & Fractals. Volume 24, Issue 3, May 2005, Pages 759–765.

[19] http://en.wikipedia.org/wiki/Histogram

[20] Karl Pearson (1895), "Contributions to the Mathematical Theory of Evolution II, Skew Variation in Homogeneous Material". Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 186: 343–414.

[21] Xu Shujiang Wang Yinglong, Guo Yucui Wang Cong, "A Novel Chaos-based Image Encryption Scheme", International Conference on Information Engineering and Computer Science (ICIECS) 2009, 19-20 Dec. 2009, pages: 1- 4.

[22] http://www.waset.org/journals/waset/v3/v3-7.pdf Analysis and Comparison of Image Encryption Algorithms by Ismet Öztürk and Ibrahim Soukpinar.

[23] Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 6, June 2012, pages: 163-167.

[24] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Volume 2012 (2012), Article ID 173931, 13 pages.