Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.1112 – 1120

RESEARCH ARTICLE

Image Encryption Technique Based on Permutation and Combination

Prafull Kumar Singh, Mr. Mehtab Alam, Shikha Tyagi
Software Engineering & School Of Engineering &Technology, India
HOD, Dept. of Computer Science & Noida International University
Research Scholar
Prafullraj66@gmail.com, alam12mehtab@gmail.com

Abstract— "Combination of Encryption and Decryption for secure communication is an application". Here I am using Permutation and substitution technique to make our data more secure. It is concerned in hiding the information in secure and robust manner so that the confidentiality of the data remains. This paper also attempts to identify the requirement of good key generation algorithm and its decryption. This allows the user to choose whether or not he/she wants to encrypt the data and have it password protected and the type of algorithm to use for encryption. Every image tested with this technique showed no visual distortions. This technique of key generation used for data (image/video) authentication.

***Keywords*— "**Cryptography"," Permutation"," Combination", "Data hiding"

1. INTRODUCTION

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. As the name implies, a substitution operation involves replacing one thing with something else. In cryptography, it generally involves replacing one symbol with another symbol. For example, in the Caesar Shift Cipher, each letter of the plaintext is replaced by the letter three places further down in the alphabet (wrapping back to the beginning if the end of the alphabet is reached). A permutation is an arbitrary reordering of the members of a set. While not glaringly obvious, any permutation can be accomplished by the proper sequence of transpositions (using the strict definition, i.e., swap exactly two members).

permutation is just a mathematical term for a function $\sigma: X \rightarrow X$ that maps a finite set X onto itself, in such way that for each $y \in X$ there exists exactly one $x \in X$ such that $\sigma(x)=y$. This is also equivalent to how the term **substitution** is used in cryptography, so your question is indeed justified.

For instance, the term **Pseudo Random Permutation** denotes a function that might also have been described as a Pseudo Random Substitution (but never is).

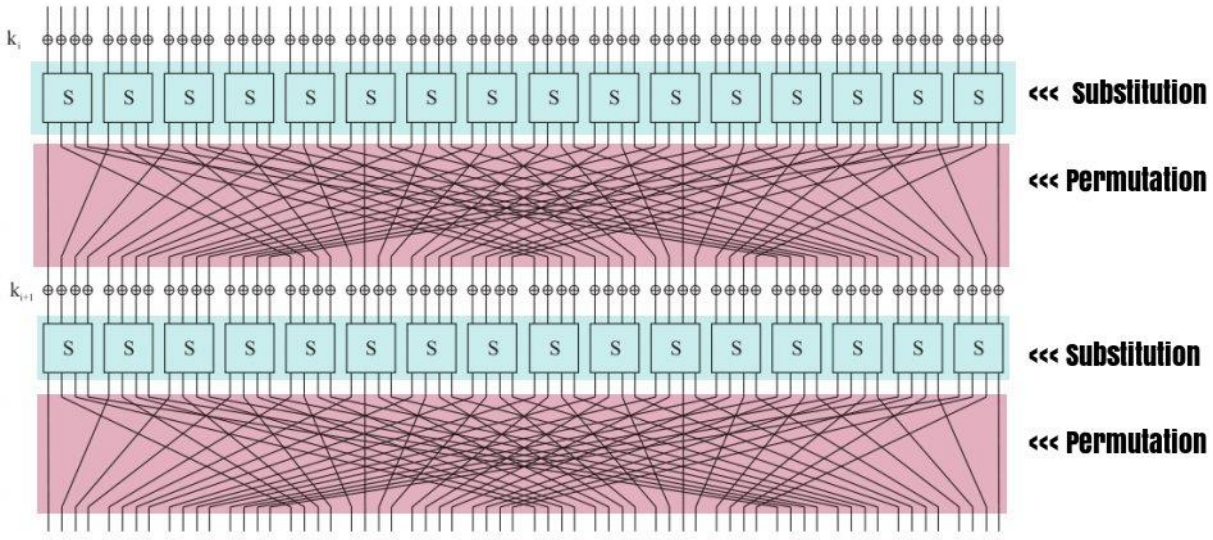
As D.W. pointed out in a comment below, the terms P-boxes (permutation boxes) and S-boxes

(substitution boxes) have a specific meaning in block cipher design. Suppose you have a P-box and a S-box that both map a bit-string of length n to another bit-string of length n. In such case the P-box can be expressed as a function $\sigma:[0..n-1]\rightarrow[0..n-1]$ that maps one index in the bit string to another, while the S-box, simply put, does more. This means that there are only $n!=\Pi ni=1i$ different P-boxes that map one bit string of length n to another, while there are $2n!-n!$ different S-boxes that map any bit string of length n to another, without being a P-box and without mapping two different inputs to the same output.

Using the term **Permutation** in the specific meaning described in the above paragraph is unambiguous within the field of block cipher design. However, I would recommend using the term **P-box**, which, to the best of my knowledge, is never used in a meaning that differs from above.

Why? Well, for instance, a block cipher designer who hypothetically decides to incorporate e.g. the RC4 key schedule for setting up the S-boxes used in a block cipher, would be technically correct to refer to the operation that sets up those S-Box as a "permutation" (because one property of such a S-box might be best understood by looking at the setup in terms of permutation decomposition). The result would clearly not be a P-box, though.

Consequently, the best answer is probably that the distinction must be clear from definitions made in the context where the terms appear. When in doubt, avoid terms that might cause confusion.



Permutation

A “P-box” is a permutation of all the bits, meaning: it takes the outputs of all the S-boxes of one round, permutes the bits, and then feeds them into the S-boxes of the next round. A good P-box has the property that the output bits of any S-box are distributed to as many S-box inputs as possible.

Substitution

An “S-box” is usually not simply a permutation of the bits. Rather, a good S-box will have the property that changing one input bit will change about half of the output bits… the so-called “avalanche effect”. An S-box will also have the property that each output bit will depend on every input bit.

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].

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 2512 (≅ 10154 possible combinations). Thus, if a computer does 1010 calculations per second, will take about 10136 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.

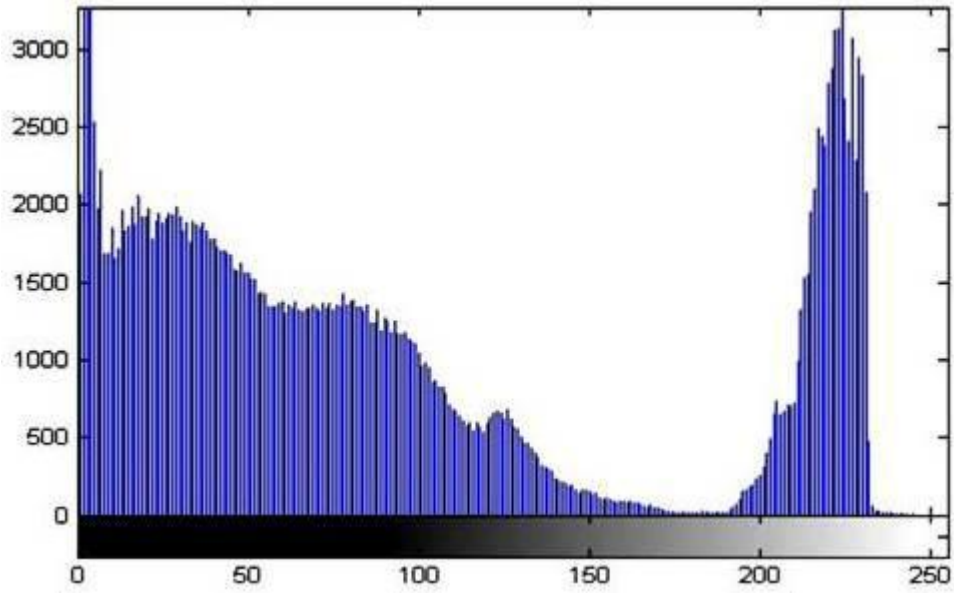


Fig 7: Histogram of an original image

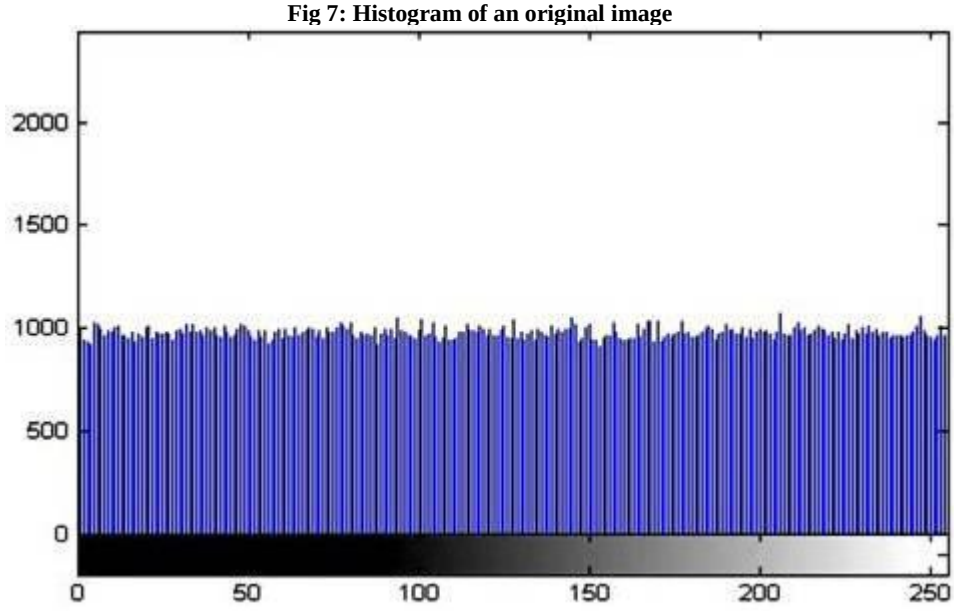


Fig 8: Histogram of Cipher Image

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).

□ □ 2 1 2 0 log ( ) (2) N i i i H(m) P(m) P m □ □ □ □ □

Where p (mi) 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⁄ 28. 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, xi and yi are two pixel pair then the correlation coefficient can be calculated by equation (6) [24].

NPCR=

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

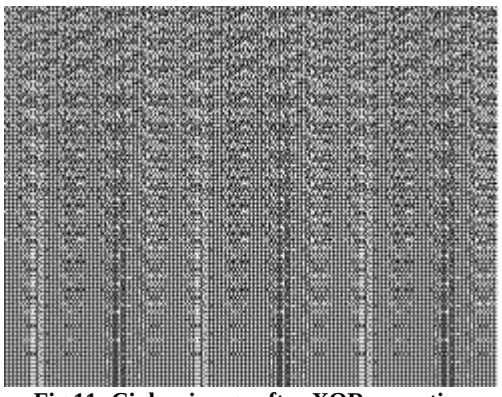


Fig 11: Cipher image after XOR operation

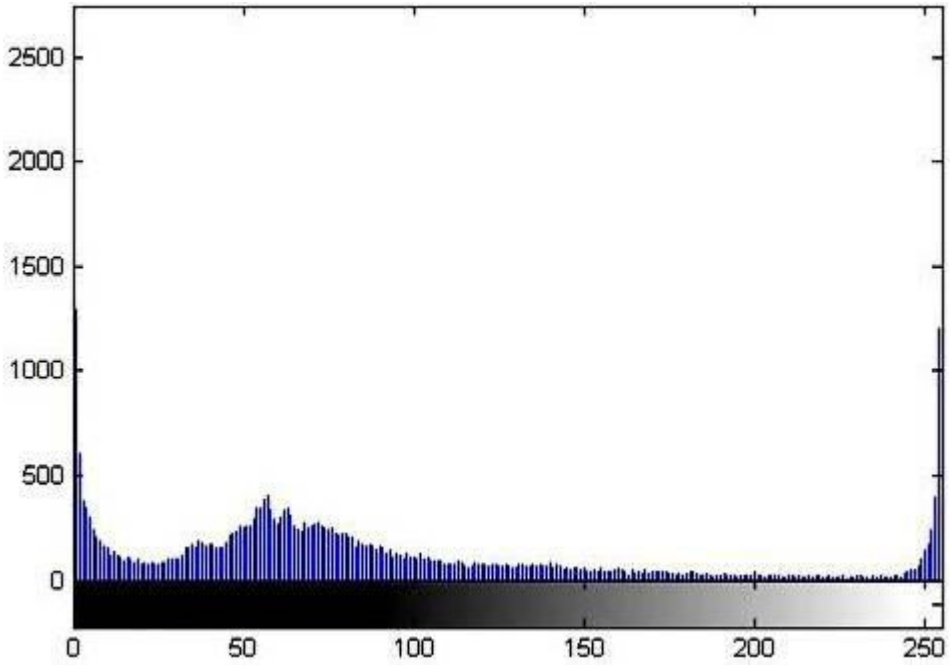


Fig 12: Histogram of the original car

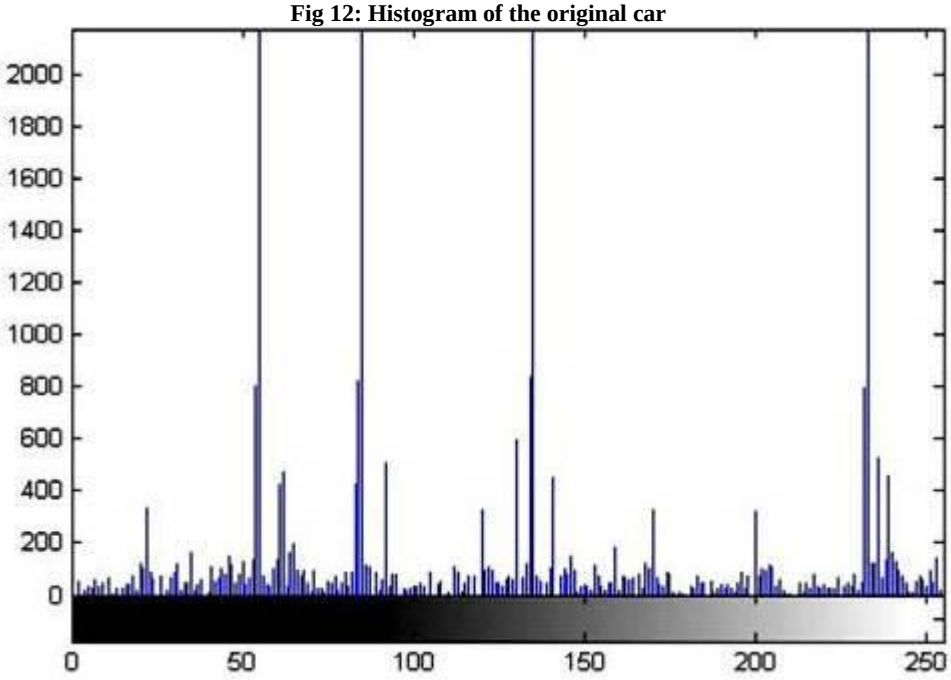


Fig 13: Histogram of Cipher

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

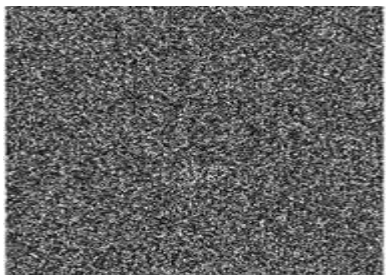


Fig 16: Cipher at iteration 15

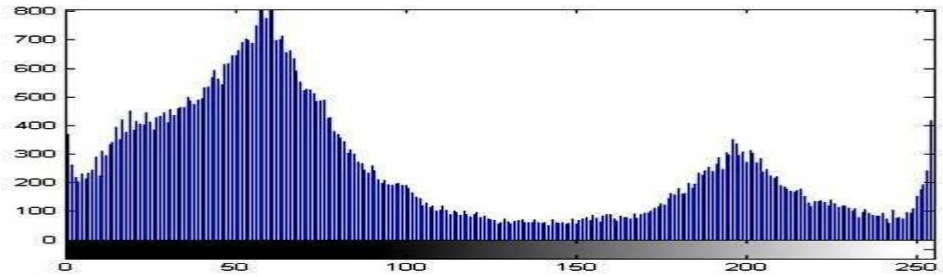


Fig 17: Histogram of dog image

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

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.

S. N	Authors	Technique Used	Key space	Key sensitivity	Correlation		Histogram	Entrophy		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
7	Proposed Algorithm	Permutation &substitution	10^{120}	High	7.43	7.996	Good	9.311	.005	99.53

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 on fusion to and Shannon's diffusion property,(5) c 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 %).

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.

