

An Analytical Survey on Different Secured Image Encryption Techniques

¹ Prabir Kr. Naskar, ² Sumit Majumdar, ³ Prasenjit Das, ⁴ Avijit Bose

^{1, 2, 3, 4} Department of Computer Science and Engineering,
MCKV Institute of Engineering
Liluah, Howrah-711204, West Bengal, India

Abstract – In modern age, secret image transmission over internet is an important issue. So, protections of secret images are major challenge during transmission over internet. Encryption is one of the popular techniques to protect secret images. Modern cryptography provides essential techniques for securing information and protecting multimedia data. Although traditional encryption techniques are not suitable for protection of secret images due to bulk data capacity and high correlation among neighboring pixels. In recent years, many popular encryption techniques have been emerged and many image encryption methods have been used to protect confidential image data from unauthorized access. This paper is an analytical survey of popular secured image encryption techniques from which researches can get an idea for efficient techniques to be used.





Keywords - Image encryption, decryption, multilevel image encryption, encryption by random grids, total shuffling.

1. Introduction

In current scenario, providing security to secret information is a challenging issue. The high growth in the networking technology leads to a common culture for interchanging of the data very drastically. So information has to be protected during transmission over internet. There are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, cryptography deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange. Steganography is a technique for hiding and extracting information which to be conveyed using a carrier signal and watermarking is a technique for hiding proprietary information in the perceptual data. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The

evolution of encryption is moving towards a future of endless possibilities. Everyday, new methods of encryption techniques have been discovered. This paper shows some of those recent existing encryption techniques and their security issues. Some of the encryption algorithms are designed for specific type of digital data. A digital data may be text, audio or an image. Presently, images are used as a secret data in various sectors like defense, medical, satellite communication, and industry. Characteristic of an image data is completely different for text data because an image contains huge data, and all data are highly correlated. Also an image data contains high redundancy. The conceptual difference between text and image is shown in table-1.

Table-1. Difficulties of image encryption over text

Type	Secret Data	Encrypted data	Remarks
Text	"CSEMCKVIE"	"DTFNDLWJF"	Completely different
Image (RGB)	 Pixel (P_1) = (24, 45, 233)	 Pixel (P_2) = (10, 65, 198)	P_1 and P_2 are completely different, but visually they look similar.
Image (Gray)	 Pixel (P_1) = (87)	 Pixel (P_2) = (114)	P_1 and P_2 are completely different, but visually they look similar.

In table-1, the value of a 24-bit image pixel is $P_1 = (r, g, b) = (25, 45, 233)$. The intensity value of blue is high as compare to red and green, so the color is shown as blue. After changing each byte of P_1 , the pixel value becomes

$P_2 = (r, g, b) = (10, 65, 198)$ and visually we detect P_2 as closer to blue, because the value of blue is higher than red and green. Although, P_1 and P_2 are completely different. In the literature, there are various strong encryption algorithms like DES[1], Triple-DES[2], AES[3], RSA[4] etc. Moreover, traditional algorithms are not suitable for images due to some intrinsic features like bulk data capacity and high correlations among pixels. Consequently, the traditional encryption algorithms need longer time to directly encrypt the image data, the second, is the encrypted image slightly reveals the original image. Fig-1.b shows an encrypted image which is slightly closer to secret image (fig.1.a).

Nowadays when more and more sensitive information are stored in computers and transmitted over the internet, security and safety of information should be ensured. Image is also an important part of secret information. Therefore it's very important to protect images from unauthorized access. In the literature, there are many encryption schemes proposed for protecting secrecy of images from unauthorized access. Some of the existing techniques are described in next section.

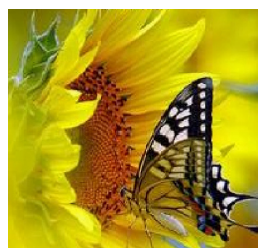


Fig-1.a.Secret image

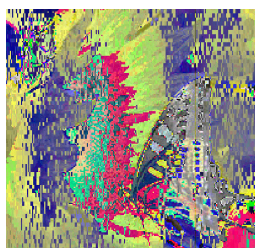


Fig.1.b. Encrypted image

Figure-1. Visually similar encrypted & secret image

2. Literature Survey

This section shows some secure image encryption techniques and a short description of various techniques used for image encryption.

2.1 Color Image Encryption using Double Random Phase Encoding^[5]

Shuqun Zhang and Mohammad A. Karim [5] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the

color images are recovered by converting the decrypted indexed images back to their rgb formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods.

2.2 A New Mirror-Like Image Encryption Algorithm and it's VLSI Architecture^[6]

Jiun-In Guo and Jui-Cheng Yen[6] have proposed an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system. An image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step-1 determines a 1-D chaotic system and its initial point $x(0)$ and sets $k = 0$. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system. Steps-4, 5, 6, and 7 rearrange image pixels using swap function according to the binary sequence.

2.3 Lossless Image Compression and Encryption using SCAN^[7]

S.S. Maniccam and N.G. Bourbakis[7] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodology to generate a wide range of scanning paths or space filling curves.

2.4 A New Encryption Algorithm for Image Cryptosystems^[8]

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen[8] have used vector quantization for designing better cryptosystem for images. The scheme is based on vector quantization, which is one of the popular image compression techniques. In vector quantization (VQ), firstly the images are decomposed into vectors and then sequentially encoded vector by vector. The goals of this approach are to design a high security image cryptosystem and to reduce computational complexity of the encryption and decryption algorithm.

2.5 A Technique for Image Encryption using Digital Signatures^[9]

Sinha and Singh[9] have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as Bose-Chaudhuri Hochquenghem (BCH) code. At the

receiver end, after decrypting the image, the digital signature can be used to verify the authenticity of the image.

2.6 Multilevel Image Encryption by Binary Phase XOR Operations^[10]

Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chul, Ha Wmn Lee, and SmJmng Kim[10] have proposed an algorithm which is multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same gray level multi-level image is divided into binary images. Then binary images are converted to binary phase encoding and then these images are encrypted with binary random phase images by binary phase XOR operation. Encrypted gray images are generated by combining each binary encrypted image. Decryption process is done with Joint Transform Correlator (JTC) and verified the scheme by computer simulation.

2.7 Image Encryption using Chaotic Logistic Map^[11]

Pareek, Patidar and Sud[11] have proposed a chaotic logistic map based image encryption in order to meet the requirements of the secure image transfer. In encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weightage to all of its bits. Further, in the encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting each block of sixteen pixels of the image. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

2.8 A Modified AES Based Algorithm for Image Encryption^[12]

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki[12] have analyzed the Advanced Encryption Standard (AES), and in their image encryption technique, they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance.

2.9 Image Encryption by Random Grids^[13]

S. J. Shyu[13] has proposed an image encryption by random grids. A random grid in this paper is a

transparency comprising a two-dimensional array of pixels that are either transparent or opaque determined in a totally random way. The algorithms is designed by using random grids to accomplish the encryption of the secret gray-level and color images in such a way that neither of the two encrypted shares alone leaks the information of the secret image, whereas the secret can be seen when these two shares are superimposed. The decryption process is done by our visual system and no computation is required. As compared to the approaches in visual cryptography, this algorithm does not need the basis matrices to encode the shares so that the problem of pixel expansion exists no more; that is, the sizes of the secret image and the encrypted shares are the same.

2.10 Image Encryption using Block-Based Transformation Algorithm^[14]

Mohammad Ali Bani Younes and Aman[14] have used a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image is divided into blocks, which are rearranged into a transformed image using a transformation algorithm, and then the transformed image is encrypted using the Blowfish algorithm. Their results show that the correlation between image elements is significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

2.11 An Image Encryption Approach using A Combination of Permutation Technique Followed by Encryption^[15]

Mohammad Ali Bani Younes and Aman Jantan[15] have introduced a new permutation technique based on the combination of image permutation and a well known encryption algorithm called Rijndael. The original image is divided into 4×4 blocks, which are rearranged into a permuted image using a permutation process, and then the generated image is encrypted using the Rijndael algorithm. The results show that the correlation between image elements is significantly reduced and higher entropy is achieved by combining techniques.

2.12 Image Encryption Based on A New Total Shuffling Algorithm^[16]

Tiegang Gao and Zengqiang Chen[16] have proposed image encryption scheme, which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-

image and the cipher-image. Authors have shown experimental results to demonstrate the new image total shuffling algorithm has a low time complexity and the suggested encryption algorithm of image has the advantages of large key space and high security, and moreover, the distribution of gray values of the encrypted image has a random-like behavior.

2.13 A New Image Encryption Approach using Combinational Permutation Techniques^[17]

A new approach for image encryption using a combination of different permutation techniques is proposed by Mitra et al. [17]. The main idea behind the present work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. Authors have shown an approach for a random combination of the aforementioned permutations for image encryption. The permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. A random combination method employing all the three techniques thus is observed to be useful for tactical security applications, where protection is needed only against a casual observer.

2.14 Digital Image Encryption Algorithm Based on Chaos and Improved DES^[18]

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zhengejun, Nie Xuan and Dai Wei-di [18] have researched on the combinations of image encryption algorithm like chaotic encryption, Des encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer has been used; this sequence is applied on RGB images chaotically, then double time encryption is carried out with improvement DES. This algorithm achieve high security and the encryption speed.

2.15 Modulo Image Encryption with Fractal Keys^[19]

Valerij Rozouvan[19] has proposed a modulo operation based encryption technique. The technique is a one-to-one encryption-decryption single key algorithm. Fractal images are used as a source of randomness to generate strong keys. The use of this method is verified, both in the single image encryption-decryption, and in a real-time streaming application. The described algorithm provides a

mechanism for controlling the strength of the keys. The advantages of the proposed method are discussed. A video setup is built and GUI software implemented to practically test this method. Numerical results of the test are provided and analyzed. Overall, the theoretically anticipated results are achieved, and the algorithm proven to be adept for real world cryptographic applications.

2.16 An Image Encryption Scheme with A Pseudorandom Permutation Based on Chaotic Maps^[20]

Ji Won Yoon and Hyoungshick Kim[20] has proposed a new image encryption algorithm using a large pseudorandom permutation which is jointly generated from small permutation matrices based on chaotic maps. Many research efforts for image encryption schemes have elaborated for designing nonlinear functions since security of these schemes closely depends on inherent characteristics of nonlinear functions. It is commonly believed that a chaotic map can be used as a good candidate of a nonlinear component for image encryption schemes. In this paper authors use the random-like nature of chaos, which is effectively spread into encrypted images by using the permutation matrix. The authors have shown experimental results to prove the proposed encryption scheme provides comparable security with that of the conventional image encryption schemes based on Baker map or Logistic map.

2.17 Image Encryption using Affine Transform and XOR Operation^[21]

Amitava Nag et al.[21] have introduced a new algorithm using affine transform and were based on shuffling the image pixels. It was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

2.18 A Novel Algorithm for Image Encryption by Integrated Pixel Scrambling Plus Diffusion [IISPD] Utilizing Duo Chaos Mapping Applicability in Wireless Systems^[22]

G. A. Sathish Kumar, K. Bhoopathy Bagan, V. Vivekanand[22] have proposed a new method for image encryption by integrated pixel scrambling plus diffusion technique [IISPD]. The algorithm makes use of full

chaotic property of logistic map and reduces time complexity. The algorithm calculates the permuting address for row by bit xoring the adjacent pixel values of original image. Similarly, the algorithm calculates the permuting address for column by bit xoring the adjacent pixel values of original image. Therefore, the new techniques does not require the knowledge of probability density function of the chaotic orbits a priori, thus it reduces the complexity of the proposed technique. The diffusion is performed after scrambling and is based on two chaotic maps. Therefore, the key space and security of the algorithm is increased. It also has higher key space, and higher degree of scrambling.

2.19 An Improved Image Encryption Method Based on Total Shuffling Scheme^[23]

Yan Shen, Guoji Zhang, XCuan Li, Qing Liu[23] have proposed an improved image encryption method based on permutation-diffusion architecture and total shuffling scheme. In the permutation process, the P-box, which makes every image shuffle the position of pixels by its own P-box, depends on the plain-image. In the diffusion process, the keystream is related to the plain-image directly and a more secure feedback is employed to change the number of iterations of the chaotic map. Moreover, a reverse diffusion process is added to protect the final cipher-image. From experimental results of statistical analysis, information entropy analysis and sensitivity analysis, it is demonstrated that the improved algorithm is more secure and reliable than the original one and it can avoid various categories of attack.

2.20 A Novel Image Encryption Technique using Multi-Wave Based Carrier Image^[24]

H. T. Panduranga and S. K. Naveen Kumar[24] have proposed a novel technique for image encryption based on carrier image. Here, pixels of a carrier image are created by amplitude values of multiple sine waves generated by alphanumeric password. Finally this carrier image is added with original image to obtain encrypted image. Decryption process involves the same procedure to create carrier image and it is added with the encrypted image to get original (decrypted) image. Experiment is conducted for various combinations of multiple waves to generate various patterns in carrier image.

2.21 A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based on Sorting Group-Wise of RGB Values and Explosive Inter-Pixel Displacement^[25]

Many researchers has proposed contrastive methods to encrypt images but correlation between pixels RGB value

play a imperative part to guess for original image. So, Goel et al.[25] have proposed an image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. Experimentally it has shown that pixel rearrangement is enough from image encryption point of view but to send image over open network; inter-pixel displacement algorithm is applied to dispense more armament to image before transmission.

2.22 Image Encryption Based on Bit-Plane Decomposition and Random Scrambling^[26]

Qiudong Sun et al.[26] have proposed a general random scrambling method which is stable scrambling degree than the classical method Arnold transform. At first, it decomposes a gray image into several bit-plane images. Then this technique shuffles them by a random scrambling algorithm separately. Lastly, this technique merge the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image. Due to each bit-plane image is scrambled using different scrambling random sequences, the bits situated at the same coordinates in different bit-planes most likely not to stay on the original positions. For every pixel, it's all bits of gray level, therefore, may be come from those pixels located in different positions. Consequently, the reconstructed gray levels of image are changed ineluctable. Method can do both positions exchange scrambling and gray level change scrambling at the same time.

2.23 Rapid Encryption Method Based on AES Algorithm for Gray Scale HD Image Encryption^[27]

Salim M. Wadi and Nasharuddin Zainal[27] have proposed a new HD gray scale image using Advanced Encryption Standard (AES)[3]. Advanced Encryption Standard (AES) is a famous and strong encryption algorithm which has several advantages in data ciphering. However, AES suffer from some drawbacks such as high computations, pattern in ciphered images, and hardware requirement. Those problems are more complicated when AES algorithm will use for images ciphering especially the HD images. Some modifications were proposed to enhance the performance of AES algorithm in terms of time ciphering and pattern appearance. First modification is decreasing the number of rounds to one while the second modification is replaced the S-box with new S-box to decrease the hardware requirements. Applying AES in one of the ciphering mode solves the pattern appearance

problems. The experimental results indicate that the proposed modifications make AES algorithm faster while fulfill the security requirements.

2.24 A Secure Symmetric Image Encryption Based on Linear Geometry^[28]

P. K. Naskar et al.[28] have proposed a symmetric encryption technique based on linear geometry. Though the basic idea is based on block ciphering using the linear geometry for ciphering. The ciphered bytes are again shuffled among N positions (N is size of secret file in bytes). The scheme is basically combination of substitution as well as transposition techniques, which provides better protection for secret image. It may be mentioned that there is no change in size after encryption. The scheme has strong key sensitivity and resists statistical attacks like number of pixel change rate, unified average changing intensity etc. The scheme is also tested using different images to establish that the technique is quite robust and has a great potential to meet the security needs for digital images.

2.25 An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves^[29]

Yuanyuan Sun et al.[29] have proposed an effective image encryption technique to protect image security. A novel image encryption algorithm combining Julia sets and Hilbert curves is used to encrypt an image. The algorithm utilizes Julia sets' parameters to generate a random sequence as the initial keys and gets the final encryption keys by scrambling the initial keys through the Hilbert curve. The final cipher image is obtained by modulo arithmetic and diffuse operation. In this method, it needs only a few parameters for the key generation, which greatly reduces the storage space requirement. Moreover, because of the Julia sets' properties, such as infiniteness and chaotic characteristics, the keys have high sensitivity even to a tiny perturbation. The experimental results have shown that the algorithm has large key space, good statistical property, high sensitivity for the keys, and effective resistance to the chosen-plaintext attack.

2.26 A Secure Symmetric Image Encryption Based on Bit-Wise Operation^[30]

P. K. Naskar and A. Chaudhuri[30] have proposed a symmetric image encryption based on bit-wise operation (XORing and Shifting). The basic idea is block ciphering technique to cipher the secret bytes, after that ciphered bytes are again shuffled among N positions (N is the size of secret file). The scheme is combination of substitution

as well as transposition techniques which provides additional protection of the secret data. The substitution and transposition are done using dynamic substitution box (SBOX) and transposition box (TBOX) which are generated using the secret key and made to vary for each block during ciphering. The size of encrypted data is same as the size of secret data and the scheme has been tested using different images. Authors have shown the security analysis such as key sensitivity analysis, statistical analysis, and differential analysis to prove the strength of the scheme against crypto analysis.

2.27 Image Encryption Based on Singular Value Decomposition^[31]

Nidhal et al.[31] have proposed a novel secure encryption method for image encryption is presented in this study. The proposed algorithm based on using singular value decomposition (SVD). In this study we start to scramble the image data according to suggested keys (two sequence scrambling process with two different keys) to finally create two different matrices. The diagonal matrix from the SVD will be interchanged with the resulted matrices. Another scrambling and diagonal matrices interchange will apply to increase the complexity. The resulted two matrices combine to one matrix according to predefined procedure. The encrypted image is a meaningful image. The suggested method tested with many images encryption and gives promised results.

2.28 An Image Encryption Scheme Based on Bit Circular Shift and Bi-Directional Diffusion^[32]

Ruisong et al.[32] have proposed a novel image encryption based on chaotic system. This scheme utilized one tent map to generate a pseudorandom sequence and then shift the bits of the expanding 0-1 image circularly so as to shuffle the image gray values. Moreover generalized Arnold maps and Bernoulli shift maps are applied to produce two pseudo-random gray value sequences and then diffuse the gray values bi-directionally, which resisted the scheme from differential attack efficiently. The bit circular shift process and diffusion processes greatly confused the statistical nature between plain-images and cipher images. The scheme used a large key space which is useful to frustrate brute-force attack efficiently.

2.29 A Novel Double-Image Encryption Scheme Based on Cross-Image Pixel Scrambling in Gyrator Domains^[33]

Jun-Xi Chen et al.[33] have proposed a novel double-image encryption scheme based on cross-image pixel

scrambling in gyrator domains. The two input images are firstly shuffled by the proposed cross-image pixel scrambling approach, which can well balance the pixel distribution across the input images. The two scrambled images will be encoded into the real and imaginary parts of a complex function, and then converted into gyrator domains. An iterative architecture is designed to enhance the security level of the cryptosystem, and the cross-image pixel scrambling operation is performed to the real and imaginary parts of the generated complex encrypted data in each round. Numerical simulation results prove that a satisfactory and balanced security performance can be achieved in both channels.

3. Conclusions

Nowadays, providing security of a secret image is very important. Although, Image encryption is completely different from text encryption. This survey paper shows some important encryption techniques in the span of more than 14 years (1999-2014) and those techniques are studied and analyzed in order to make familiar with the various encryption algorithm used in encrypting the image. To sum up, all the techniques are useful for real time encryption and each technique is unique in its own way, which might be suitable for image as secret data. Every day new encryption technique is developing therefore fast, robust and secure conventional encryption techniques will work with high rate of security.

Acknowledgments

We are thankful to Department of Computer Science and Engineering, MCKVIE for providing moderate lab facilities and infrastructure to carry our research work successfully.

References

- [1] National Bureau of Standards, "Data Encryption Standard", FIPS Publication 46, 1977.
- [2] NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67.
- [3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard", Dr. Dobb's Journal, 2001.
- [4] Rivest, R.; A. Shamir; L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 (2), 1978, pp.120-126.
- [5] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters, 1999, vol. 21(5), pp.318-322.
- [6] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, 2000, vol.10 (2), pp.236-247.
- [7] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition (34), 2001, pp.1229- 1245.
- [8] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems ", The Journal of Systems and Software (58), 2001, pp.83-91.
- [9] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, 2003, vol-218, pp.229-234.
- [10] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, SmJmng Kim, "Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding, 2003, vol.3.
- [11] N. K. Pareek, V. Patidar, K. K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing 24, Elsevier, 2006, pp.926-934.
- [12] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering, 2007, vol.01(3), pp.735-740.
- [13] Shyong Jian Shyu, "Image encryption by random grids", Pattern Recognition 40, 2007, pp.1014-1031.
- [14] Mohammad Ali Bani Younes, Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 2008, vol.35(1).
- [15] Mohammad Ali Bani Younes, Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, 2008, vol.8(4), pp.191-197.
- [16] Tiegang Gao, Zengqiang Chen, "Image encryption based on a new total shuffling algorithm", Chaos, Solitons & Fractals, Elsevier, 2008, vol.38(1), pp.213-220
- [17] A. Mitra, Y. V. Subba Rao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", World Academy of Science, Engineering and Technology, 2008, vol.2, pp.812-816.
- [18] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, "Digital image encryption algorithm based on chaos and improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009, pp.474-479.
- [19] Valerij Rozouvan, "Modulo image encryption with fractal keys", Optics and Lasers in Engineering 47, 2009, pp.1-6.
- [20] Ji Won Yoon, Hyounghick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", Commun Nonlinear Sci Number Simulat, Elsevier, 15, 2010, pp.3998-4006.

- [21] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation", International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), IEEE, 2011, pp.309-312.
- [22] G. A. Sathish Kumar, K. Bhoopathy Bagan, V. Vivekanand, "A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems", Procedia Computer Science 3, 2011, pp.378-387
- [23] Yan Shen, Guoji Zhang, XCuan Li, Qing Liu, "An Improved Image Encryption Method Based on Total Shuffling Scheme", Advances in CSIE, Springer-Verlag, 2012, vol.2, AISC-169, pp.643-650.
- [24] H. T. Panduranga, S. K. Naveen Kumar, "A Novel Image Encryption Technique using Multi-Wave Based Carrier Image", International Conference on Modeling Optimization and Computing (ICMOC), Procedia Engineering, 2012, vol-38, pp.2998-3004.
- [25] Amnesh Goel, Nidhi Chandra, "A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based on Sorting Group-Wise of RGB Values and Explosive Inter-Pixel Displacement", International Journal of Image, Graphics and Signal Processing, 2012, vol.2, pp.16-22.
- [26] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University, 2012, IEEE, vol. 09, pp.2630-2633.
- [27] Salim M. Wadi, Nasharuddin Zainal, "Rapid Encryption Method based on AES algorithm for Gray Scale HD Image Encryption", ICEEI 2013, Procedia Technology, 2013, vol.11, pp.51-56
- [28] P. K. Naskar, A. Chaudhuri, A. Chaudhuri, "A secure symmetric image encryption based on linear geometry", Applications and Innovations in Mobile Computing (AIMoC), IEEE, 2014, pp.67-74.
- [29] Yuanyuan Sun mail, Lina Chen, Rudan Xu, Ruiqing Kong, "An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves", PLOS ONE, Vol-9, Issue-1, 2014.
- [30] P. K. Naskar, A. Chaudhuri, "A Secure Symmetric Image Encryption Based on Bit-wise Operation", International Journal of Image, Graphics and Signal Processing (IJIGSP), 2014, vol.6(2), pp.30-38.
- [31] Nidhal K. EI Abbadi, Adil Mohamad, Mohammed Abdul-Hameed, "Image Encryption based on Singular Value Decomposition", Journal of Computer Science 10(7), 2014, pp.1222-1230.
- [32] Ruisong Ye, Shaojun Zeng, Peiqian Lun, Junming Ma, Chuting Lai, "An Image Encryption Scheme based on Bit Circular Shift and Bi-directional Diffusion", International Journal of Information Technology and Computer Science, 2014, pp.82-92.

- [33] Jun-xi Chen, Z-liang Zhu, Zhengjun Liu, Chong Fu, Li-bo Zhang, Hi Yu, "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains", Optics Express, Optical Society of America, 2014, vol.22(6), pp.7349-7361.



Mr. Prabir Kr. Naskar (B.Tech in Computer Science & Engineering, M.Tech in Computer Technology) is presently working as Assistant Professor in the Department of Computer Science & Engineering, MCKV Institute of Engineering, West Bengal, India for last three years. His current research interests include: cryptography, information sharing, steganography, watermarking and image processing.



Mr. Sumit Majumdar (B.Tech in Computer Science & Engineering, M.E in Computer Science and Engineering) is presently working as Assistant Professor in the Department of Computer Science & Engineering, MCKV Institute of Engineering, West Bengal, India for last four years. His current research interests include: Pattern recognition, Image processing, cryptography and watermarking.



Mr. Prasenjit Das is Assistant Professor in the Computer Science and Engineering Department of MCKV Institute of Engineering. He received the M.C.A. and M.Tech. Degree from West Bengal University of Technology. His current research focuses on the data mining, optimization techniques and image processing.



Mr. Avijit Bose (B.Tech in Computer Science and Engineering, M.Tech in Information Technology) is presently working as Assistant Professor in the Computer Science and Engineering Department of MCKV Institute of Engineering for last ten years. He is the member of IEEE. His current research focuses on the Network security, cryptography, and wireless mobile network.