*Journal of Information Sciences and Computing Technologies(JISCT)*
*ISSN: 2394-9066*

SCITECH
RESEARCH ORGANISATION|

Volume 5, Issue 3
May 28, 2016

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com/journals

# Recent Trends in Image Encryption: A Review

Ibrahim M. Harram[1], Mala U. M. Bakura[2], Ali M. Mohammed[3] and Abdullahi M. Kire[4]
[1,3,4] *Department of Elect.& Electronics Engineering Technology, The Federal Polytechnic, Damaturu, Yobe State, Nigeria*
[2]*Department of Electrical and Electronics Engineering, University of Maiduguri, Borno State, Nigeria*

## Abstract.

*Security of multimedia data is gaining acceptance owing to the growth and acceptability of images in various applications and in telecommunication. Encryption is one of the ways to ensure the security of images as they are used in many fields such as in secure medical imaging services, military intelligence, internet and intranet communication, e-banking etc. These images are stored or transmitted through a network; hence the security of such image data is important. In this work, recently developed encryption techniques are studied and analyzed to promote further development of more encryption methods to ensure additional security and versatility. All the techniques reviewed came into existence within the last five years (2011-2015) and are found to be useful for the present day encryption applications. Each technique is unique in its own way, which might be suitable for different applications. As time goes on, new encryption techniques are evolving. Hence, fast and secure conventional encryption techniques will always be needed in applications requiring high rate of security.*

## I. Introduction

Image information, as different from the text data, has larger amount of data, higher redundancy and stronger correlation between pixels. Traditional encryption algorithm such as RSA, DES etc., cannot be directly used for image encryption due to certain reasons. One of the reasons is that the image size is larger than that of text, so the traditional cryptosystems take much time to directly encrypt the image data. The other reason is that the decrypted text must be equal to the original text. However, this requirement is not very necessary for image as a decrypted image containing small distortion is acceptable due to human perception.

Image encryption techniques try to convert original image to another image that cannot be easily understood, thereby keeping it confidential between users. In other word, it is essential that nobody, apart from the sender and receiver, can get to know the content of the encrypted image without a key for decryption. Special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to achieve such a task, different image encryption techniques have been developed.

# II. Literature Review

The following data encryption techniques have recently been developed and are gaining wider acceptance in data security applications.

### 1. A Secure Symmetric Image Encryption Based on Bit-wise Operation

Naskal and Chaudhuri (2014) presented a symmetric image encryption based on bit-wise operation (XORing and Shifting) to process a block (size of each block is 4 bytes) of the secret bytes. The ciphered bytes are shuffled among N positions (N is the size of secret file). The scheme uses combination of substitution as well as transposition techniques to provide additional protection of the secret data. 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 the ciphering process. Different images formats have been put to test and the image sizes before and after encryption are the same. It is equally applicable for any digital file (e.g. text, image and audio etc.). The key for the proposed cryptosystem is very large which provides better security against brute-force attack. Moreover, key sensitivity analysis, statistical analysis and differential attack analysis prove the high acceptability of the proposed algorithm.

### 2. 2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation

In the work of Debbarma et al, (2013) a new 2-D chaos based lossless image encryption method is presented. The method employs user key based encryption and decryption with confusion and diffusion processes guided by user key. The method generates large key space which resists any brute force attack. In spites of this, the algorithm is simple enough to consume fewer amounts of computations resulting fast processing. Statistical analysis of this method has been performed the results shows that the proposed method is secure enough and is suitable for encrypting all type of images, e.g. RGB images (colored images), Gray scale images, and Binary images. The 2-D chaos is generated separately for red, green, and blue components of RGB image. After chaos generation, encrypted image of R, G, and B components are placed at their respective places. If image is gray scale or binary, then there is only one plane to encrypt (instead of 3 for RGB images) by chaos development. The scheme is implemented in MATLAB for computer simulations. Image encryption is done by eight cascaded iteration of confusion and diffusion. This method has drastically disrupted statistical properties and also neutralizes histogram of R, G, and B components of image. Its cryptographic qualities have been evaluated through different statistical analyses and it supports portability architecture because only integers are used during the encryption/decryption processes. It is concluded that the proposed algorithm for image encryption is useful for application of image encryption and is based on guiding user.

## 3. A Cryptographic Image Encryption Technique for Facial-Blurring Of Images

In this work, Kester Q. (2013) proposes an image encryption technique that will make it possible for selected facial or sensitive area to be encrypted based on RGB pixel shuffling of an m*n size image. Protection of faces and sensitive areas in pictures and videos of people in connection with sensitive information, activism, abused cases and others on public broadcasting media and social net-works is very important. On social networks like YouTube, Face book, Twitter and others, videos are being posted with blurring techniques of which some of them cannot be recovered. Most blurring techniques used can easily be recoverable using off-the-shelf software. The ones that are difficult to be recovered also can easily be used by abusers and other wrong doers. This will make it difficult for off-the-shelf software to restore the encrypted image and also make it easy for the law enforcement agencies to reconstruct the face back in case the picture or video is related to an abuse case. The implementation of the encryption method was done using MATLAB. The facial selected portion of the image used will have their RGB colors extracted and then encrypted to have a ciphered image portion. The ciphering of the image in this work was done by using the RBG pixel values of the selected portion of the images. There are no changes of the bit values and there is no pixel expansion at the end of the encryption process. Instead, the numerical values are transposed, reshaped and concatenated with the RGB values shifted away from its respective positions and the RGB values interchanged in order to obtain the cipher image. This implies that, the total change in the sum of all values in the image is zero. The image is looked at as a decomposed version in which the three principal components which forms the image are chosen to act upon by the algorithm. With the proposed method in this work, the shuffling of the image was ultimately done by solely displacing the RGB pixels and also interchanging the RGB pixel values. The pixel displacement and reshuffling of the image in steps between the processes has proved to be really effective. Transposition and displacement technique further makes the operation algorithm to be resistive to linear deblurring algorithms and other methods of fixing distorted pixels within images. With this approach, it will be difficult for any image deblurring technique using off-the-shelf software to restore the image back to its initial phase.

## 4. A New Fuzzy PN Codes Based Color Image Encryption Technique

In this paper, El-Khamy et al, (2012) works on a new method for generating pseudo-random image encryption system using 4 binary sequences generated using a fuzzy PN bit generator developed by the authors to encrypt the image pixels is proposed. According to these sequences, each pixel color byte value will be rotated as bits in right or left direction. Some bits, after rotation process, the pixel color will be XOR-ed by one of the binary sequences developed to obtain a highly encrypted image. A learning procedure is applied to copy the behavior of real random source. The system generates pseudorandom binary sequences. The generated fuzzy binary sequences successfully pass all standard randomness tests and their length can be made arbitrary long. Such sequences are suitable for data encryption and secure direct-sequence (DS) spread-

spectrum (SS). Although the generated codes from the fuzzy binary generator appear to be random and enjoy most of the properties of random codes, they are deterministic. In other words, they can be exactly regenerated by fixing the parameters of the fuzzy random number generator. The system is used for color images, and can be easily adopted for gray-scale images. The simulation results proves that the system provide high disorder appearance for the encrypted image with high dependency on 4 sequences. The encryption system is image content dependent, which provide an advantage in the security level.

## 5. An Image Encryption and Decryption Techniques Using Two Chaotic Schemes

Sharma et al, (2014) developed an image encryption and decryption scheme based on two chaotic systems. The scheme combines the spatial – domain encryption of digital images and the traditional stream cipher technology. The very wide encrypting space is the main advantage of using two chaotic systems. In addition, two chaotic sequences are easy to control and easy to generate. The encryption phase makes use of two chaotic sequences to encrypt an image and the reverse operation is carried out to recover original image in decryption phase. By combining the spatial-domain encryption of digital images and traditional stream ciphers technology, the security of the encryption scheme can be enhanced effectively. The advantage of chaos lies in its random behavior and sensitivity to initial conditions and parameter. chaos-based encryption algorithm have shown some exceptionally good properties in security, complexity, speed, computing power, computational overhead etc. There exist a close relationship between traditional cryptosystem and chaotic systems in many aspects. The chaotic systems experiences many superior dynamical properties which can analogously correspond to those required in cryptosystem. The notion of confusion in traditional cryptosystems causes plain image transforming to random cipher image such that there should be no repeated pattern in cipher image. In other words, it is very difficult to predict the final position of one point from its initial position. With larger key space and sensitive to the key, the technique can withstand against most known attacks. Hence the proposed technique can be used as effective tool for secured digital image Encryption.

## 6. An Improved Color Image Encryption Algorithm with Pixel Permutation and Bit Substitution

Abraham L. and Daniel N. (2013) work on the implementation of a color image encryption algorithm based on Rubik's cube technique. The Rubik's cube technique is used for pixel permutation and a bit substitution method based on DeoxyriboNucleic Acid (DNA) sequences are used to change the value of each pixel on the image. Then the time-stamp is appended with encrypted image, which can be used to identify the replay attack. During decryption, first the time-stamp is extracted from the encrypted image by using the shared secret key. The difference between the extracted time and the current time is taken. If that difference is within the threshold then the decryption is performed otherwise it is rejected. For performing the decryption, the time-stamp is appended with the key and the two random numbers are generated. The decryption is then performed to get the original image. Before performing these operations the system time should be

synchronized. The security of the Rubik's cube technique has improved by adding time-stamp and chaotic DNA substitution. The time-stamp is appended with the original key. So the time-stamp is specially added to produce different cipher texts by applying same key on same plain text. Also it can be used to check the replay attack. In basic Rubik's cube based approach bit substitution is not used. A chaotic bit substitution method based on DNA sequences is added for improving the security. To evaluate the performance of the algorithm, series of tests are performed. These tests include information entropy analysis, correlation analysis, analysis of (Number of Pixel Change Rate) NPCR and (Unified Average Changing Intensity) UACI values etc. The comparison results and assessments have been done and presented. From that the efficiency of the improved approach is evident. The experimental result shows that the improved scheme performs well in color images.

## 7. Hardware Software Co-Simulation of the Multiple Image Encryption Technique Using the Xilinx System Generator

The work by Panduranga et al, (2013) focuses on the implementation of multiple image encryption technique based on the Latin Square Image Cipher (LSIC). First, a carrier image that is based on the Latin Square is generated by using 256-bits of length key. The XOR operation is applied between an input image and the Latin Square Image to generate an encrypted image. Then, the XOR operation is applied between the encrypted image and the second input image to encrypt the second image. This approach consists of multiple stages. Except for the first stage, each stage is dedicated to the encryption of each input image. However, Stage 1 is dedicated for the generation of the Latin Square Image. In Stage 2, the XOR operation is applied between Input Image 1 and the Latin Square Image that was generated in Stage 1 which results in Encrypted Image 1. In Stage 2, the XOR operation is again applied between Encrypted Image 1 and Input Image 2 to produce Encrypted Image 2. Similar processes are performed up to Stage *n*, where the XOR operation is applied between Input Image *n* and Encrypted Image *n-1* to produce Encrypted Image *n*. This process is continues until the last input image is encrypted. A hardware co-simulation of the proposed multiple image encryption technique is achieved using the Xilinx System Generator (XSG). This encryption technique is modeled using Simulink and XSG Block set and synthesized onto Virtex 2 pro FPGA device. The technique was validated using the hardware software co-simulation method. The performance of the proposed approach suggests that the technique is more suitable when all the images are completely or even just slightly different.

## 8. Image Encryption using Hybrid Genetic Algorithm

In this work, Nichat and Sikchi (2013) developed a hybrid model for image encryption composed of genetic algorithm (using crossover operation) and chaotic function (similar to noise signal) is introduced. In the first stage of this technique, the number of encrypted images are constructed using secret key and chaotic function. In the next stage, these encrypted images are used as initial population for genetic algorithm. The genetic algorithm is used to obtain optimum result and in the last stage, the best cipher image is selected based on calculation of correlation coefficient and entropy. The image having lowest correlation coefficient and

highest entropy is selected as best cipher image. The entropy and correlation coefficient obtained by using this method are 7.9978 and -0.0009 respectively. Chaotic function Logistic Map and a key extracted from the plain-image are used to encrypt the image. The method mentioned is employed to produce a number of encrypted images using the plain-image. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

## 9. Image Encryption and Decryption Using Blowfish Algorithm in MATLAB

Singh P. and Singh K. (2013) works on encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. The algorithm was used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. The algorithm was designed and realized using MATLAB. The Blowfish block cipher published by Schneier in 1993 was developed to be a publicly available cryptographic algorithm with the potential to replace DES. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-OR (XOR) operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Both colour and black & white images of any size saved in tagged image file format (TIF), Bit map (bmp), Portable network graphics (PNG), Joint Photographic Experts group (JPEG), etc. can be encrypted & decrypted using blowfish algorithm. Histogram of encrypted image is less dynamic and significantly different from the respective histograms of the original image. Blowfish has no any known security weakness so far it can be considered as an excellent standard encryption algorithm.

## 10. Simulation of AES Based Data Encryption in Vb.net

The work of Harram et al, (2014) focuses mainly on the realization of data encryption using the famous Advanced Encryption Standard Algorithm in Vb.net framework. The study was based on the development of a computer oriented encryption program, using Advanced Encryption Standard (AES) that will ensure the security of data on transit. The data encryption and decryption system described and realized in this work using AES codes was aimed at improving data security and integrity. It has been programmed, tested and proved satisfactory with all the needed modifications and upgrading. AES is based on a design principle known as a substitution permutation network. It is fast in both software and hardware and it does not use a Feistel network. The AES codes inVb.NET Framework is the abstract base code that extends the properties and methods for using the AES algorithm. This code is inherited by two other classes, *AesCryptoServiceProvider* and *AesManaged*- that represent and managed the implementations of the AES

algorithm respectively. Data encryption and decryption system described and realized in this work using AES codes is aimed at improving data security and integrity. The development of such a system is imperative. The computer programmed software is also developed to suit the trend in data security.

## 11. Use of Symmetric Algorithm for Image Encryption

Brindha et al, (2014) work on image encryption using symmetric algorithm (SA) is presented. Encryption is a method to protect data against destruction by involving special algorithm and keys to transform digital data into unreadable format before transmission over the network. The Decryption keys are used to get the original digital data back from the transmitted encrypted data form. Data encryption standard (DES) is one of the symmetric algorithms. This paper presents an analysis on DES algorithm for image encryption. The proposed work was meant to reproduce the original image with no information loss. A comparative study of the DES algorithm with the present image encryption algorithms was also made. Image encryption with DES algorithm has been realized, which provides more security for data during the process of the transmission. Three different steps were used; conversion of image into byte array, byte array to string and then the string is passed for encryption in DES. The resultant final decrypted image is same as input image.

## 12. Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique

In the work of Sethi N. and Vijay S. (2013) a new chaotic digital image encryption scheme using new transformed mapped technique, Chirikov Standard Map and modified Logistic Map (Haar) is implemented. Chirikov Standard Map is used for pixel shuffling and modified Logistic Map is used for diffusion. The technique has two phases; one phase to transform the plain image and the other phase to actually encrypt the transformed image which incorporates both pixel substitution as well as pixel permutation process. In the substitution process, sub-block pixels value is modified which depends on used secret key and random sequence generated by modified Logistic Map. In permutation process, pixels position is reshuffled within sub-image by using key. The modified logistic map is used for generating the random sequence which is completed for the purpose of changing pixel values. The algorithm was compared with two methods first the combination Haar wavelet transformed with logistic mapping and second is the combination Fast Haar wavelet transform with logistic mapping and tested on the standard Lena image and other images. It was found for lena image that PSNR is 22.8% and 4.3% lower than the two methods respectively .It is said that lower PSNR makes better the encryption scheme. Similarly the MSE is also 60% and 9% higher than both the methods respectively. Various images and standard lena image were used to demonstrate the validity of the algorithm. The results of experiments show that the proposed algorithm for image cryptosystems provides no correlation between the original image and cipher image. The scheme is key sensitive and shows impressive resistance against brute force attack and statistical attack. It was concluded that the algorithm is resistant to statistical attacks and brute force attack.

### 13. Image Encryption Based on Bit-plane Decomposition and Random Scrambling

In this work, Sun Q. et al, (2012) developed a general random scrambling method was designed which has more stable scrambling degree than the classical method of Arnold transform. At first, a gray image is decomposed into several bit-plane images. They are then shuffled by a random scrambling algorithm separately. And lastly, they are merged to 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 by using different scrambling random sequences, the bits located at the same coordinates in different bit-planes are almost not appearing on the original positions when each bit-plane being scrambled separately. For each pixel, all its bits are of gray level, and therefore, may come from those pixels located in different positions. Consequently, the reconstructed gray levels of image are changed ineluctable. It is obvious that this method can do both positions exchange scrambling and gray level change scrambling at the same time.

## III. Results

The result of the review conducted is given in the table below. The technique employed in each of the works, Algorithm used, its platform of implementation and the special emphasis given are summarized. Equally important, parameters of interest in the works and whether encryption key is used are also studied and summarized.

**Table 1. Comparison of Recently Developed Encryption Methods**

| Author(s) | Technique(s) Employed | Algorithm Used | Platform of Implementation | Emphasis | Use of Key | Parameter(s) of Interest | Year of Publication |
|---|---|---|---|---|---|---|---|
| Naskal & Chaudhuri | Bit-wise Operation (XORing & Shifting) | Substitution and Transposition | Not Specified | To Enhance Security | To generate S-Box & T-Box for Transformation | Image Size | 2014 |
| Debbarma et al. | 8 Chaos Cascaded Iterations | Confusion & Diffusion | MATLAB | To Process all Image Formats | To Generate Chaos Based Iterations | Encryption Speed | 2013 |
| Kester Q. | Facial Blurring | Pixel Displacement | MATLAB | Portion of Image (Face) | Not Employed | R B G Pixel Values | 2013 |
| El-Khamy et al | Binary Sequence Generated using Fuzzy PN Bit Generator | Pseudorandom Binary Sequence | Visual Basic (Vb.net) | Colour & Grey Scale Images | Not Employed | Fractal Dimensions (fd) | 2012 |
| Sharma et al. | Combination of Two Chaotic Systems | Partial-Domain & Traditional Stream cipher | Not Specified | To Enhance Security | Not Employed | Image Pixels | 2014 |
| Abraham & Daniel | Rubik's Cube and Time-Stamp | Chaotic DNA Substitution | Not Specified | To Enhance Security & Maintain Image Size | To Extract Time-Stamp | Pixel Entropy, NPCR, UAIC and Correlation | 2013 |
| Panduranga et al. | Hardware/Software Co- Simulation | Latin Square Image Cipher (LSIC) | MATLAB | To Enhance Security | Not Employed | Multiple Image Frames | 2013 |
| Nichat & Sikchi | Logistic Mapping and Optimization | G. A. & Chaotic Functions | Not Specified | To Enhance Security | To Encrypt Image at Initial Stage | Correlation Coefficient & Entropy | 2013 |
| Singh P. & Singh K. | Blowfish Secret Key and Block Ciphers | Blowfish on Feistal Network | MATLAB | To Enhance Security & Processing Speed | Variable Key | Key & Block Sizes of Image Pixels | 2013 |
| Harram et al. | Implementation of AES in Vb.net | AES | Visual Basic (Vb.net) | To Enhance Security | Not Employed | Encryption Speed | 2014 |
| Brindha et al. | Conversion of Image to Bit-Array & to String | DES Symmetric Algorithm | MATLAB | To Enhance Security and Maintain Image Size | Key Selected at Random | Image Size and Encryption Speed | 2014 |
| Sethi & Vijay | Use of Various Mapping Techniques | Random Sequence | Not Specified | To Enhance Security and Maintain Image Size | Not Employed | PNSR | 2013 |
| Sun et al. | Decomposition of Bit Plane Images | Random Scrambling | Not Specified | To Enhance Security | Not Employed | Bit Plane | 2012 |

# IV. Conclusion

The issue of transmission and storage of images and other multimedia data is becoming more important than ever before. Since there increasing demand for information security, image encryption and decryption has become an important research area and it has broad application prospects. Research in the field of encryption has become indispensable in the present computer era. The security for the digital images has become of immense importance as the transmission of digital products over the open network occurs very frequently. To determine the appropriate encryption scheme for specific application often involves the consideration of certain characteristics such as encryption speed, memory requirement, security, data quality and magnitude.

In this paper, different data encryption techniques that are developed recently, have been studied and analyzed to promote further development of more encryption methods to ensure additional security and versatility. This is aimed at exposing the development trend and encouraging researchers to have a clear prospect of what will be expected in the near future.

# References

[1] **Abraham L. & Daniel N. (2013).** An Improved Color Image Encryption Algorithm with Pixel Permutation and Bit Substitution. *International Journal of Research in Engineering Technology* (IJRET) Vol. 2, Issue 11. eISSN 2319-1163.pp.333-338.

[2] **Brindha K., Sharma R. & Saini S. (2014).** Use of Symmetric Algorithm for Image Encryption. *International Journal of Innovative Research in Computer and Communication Engineering* (IJIRCCE) Vol. 2, Issue 5. pp.4401-4407.

[3] **Debbarma M., Kumari L. & Rajiha J. L. (2013).** 2D chaos Based Color Image Encryption Using Pseudorandom Key Generation. *International Journal of Emerging Trends & Technology in Computer Science* (IJETTCS) Vol. 2, Issue 4. pp.387-392.

*[4]* **El-Khamy S. E., Lofty M. & Ali A. H. (2012).** A New Fuzzy PN Codes Based Image Encryption Technique. *Electrical & Electronics Department, Faculty of Engineering, Alexandria University. Alexandria 21544, Egypt.*

[5] **Harram I. M., Bakura M. U. M. & Gwoma Z. M. (2014).** Simulation of AES Based Data Encryption in Vb.net. *International Journal of Recent Developments in Engineering & Technology* (IJRDET) Vol. 2, Issue 4. pp.5-9.

[6] **Kester Q.** A Cryptographic Image Encryption Technique for Facial Blurring of Images. *International Journal of Advanced Technology and Engineering Research* (IJATER) Vol. 3, Issue 3. pp. 1-7.

[7] **Naskar P. K. & Chaudhuri A. (2014).** A Secure Symmetric Image Encryption Based on Bit-Wise Operation. *International Journal of Images, Graphics and signal Processing* (IJIGSP) No. 2, pp. 30-38.

[8] **Nichat S. P. & Sikchi S. S. (2013).** Image Encryption Using Hybrid Genetic Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering* (IJARCSSE) Vol. 3, Issue 1. pp.428-431.

[9] **Pakshwar R., Tridevi V. K. & Richhariya V. (2013).** A Survey on Different Image Encryption and Decryption Techniques. *International Journal of Computer Science and Information Technologies* (IJCSIT) Vol. 4, Issue 1. pp.113-116.

[10] **Panduranga H. T., Kumar S. K. N. & Kumar H. S. S. (2013).** Hardware Software Co-Simulation of the Multiple Image Encryption Technique Using the Xilinx System Generator. *International Journal of Information Process System* (IJIPS) Vol. 9, No. 3. pp.499-510.

[11] **Sethi N. & Vijay S. (2013).** Comparative Image Encryption Methods Analysis Using New Transformed-Mapped technique. *Conference on Advances in Communication and Control system* (CACCS). Dehrandum Institute of Technology, Dehrandum-248001

[12] **Sharma V., Agnihotri H. C. & Patil C. H. (2014).** An Image Encryption and Decryption technique Using Two Chaotic Schemes. *International Journal of Research in Advent Technology* (IJRAT) Vol. 2, No. . pp.313-316.

[13] **Singh P. & Singh K. (2013).** Image Encryption and Decryption Using Blowfish Algorithm in MATLAB. *International Journal of Scientific and Engineering Research* (IJSER) Vol. 1, Issue 7. pp.150-154.

[14] **Sridevi S. S. P., KarthigaiKumar, P. Siva Mangai, N.M. and Vanathi, P.T. (2012)**. Survey on Efficient, Low-power, AES Image Encryption and Bio-cryptography Schemes. *Smart Computing Review*, vol. 2, no. 6. pp. 379-390.