International Journal of Scientific Engineering and Technology
Volume No.5 Issue No.6, pp: 346-351

ISSN:2277-1581
01 June 2016

A New Correlation Reduction Approach for Digital Image Encryption based on Switching and Pixel Explosion Techniques

Ambika oad, Himanshu Yadav, Anurag Jain
Department of Computer Science, RITS
Email: chandra.khambra@gmail.com, himanshuyadav86@gmail.com, anurag.akjain@gmail.com

Abstract— With digital India popularity, organizations are proposing numerous frameworks focusing on digital encryption techniques. Due to the ease of copying, editing, and tampering of digital documents and images has led to encrypting the information mandatory for transmission and storage. It evident that the correlation between the image pixels to its neighborhood region is high, reducing correlation between the pixels value makes it difficult to guess for the original image and thus improve the security. In this paper, we introduce a novel image encryption method which initially rearranges the image on the basis of switching gray codes and pixel explosion. The pixel explosion uses well-defined key that switches between the gray-code of the image pixels. Experimental results would show that the proposed pixel explosion is enough for partial encryption and enhances security of the data. Further, it could also support as an armament for any existing algorithm.

Index Terms— Encryption, Gray-Code, Pixel Displacement, Authentication

INTRODUCTION

In current era, as the digital India is gaining the momentum, the security associated with digital document and images is becoming an active research area. In addition, rapid developments in the modern communication system have allowed the exponential rise in data transfer across the network with ease. Now-a-days, it evident and documented that there is a significant rise in the confidentiality breach of certain sensitive data due to increase in the number of attackers. In general, most of the attackers focus on exploiting secret information as the transfer of data and information take place through internet is of high volume. As it is open-public access channel limiting the access would hamper the performance and reliability of the channel. Hence to counteract this vulnerability, many researchers have come up with efficient algorithms to encrypt the digital information before transmission and storage in open-public access channels.

Encryption is a science that deals with the transformation of data into a form that is unreadable to any viewer without the appropriate knowledge (a key or code) [1]; literally it transforms plain text into ciphers. Encryption is the science of using mathematics based transformation to encrypt or decrypt the data. Encryption is used to prevent data from the unauthorized access which reduces the probability of unauthorized access several times and only the authorized personnel's having the key is allowed to access it. The basic attention has now moved towards enhanced and secure communication. From all of these the information security is most leading area of research. The system in any condition should be secure enough to restrict any kind of unauthorized access and only the authorized personnel should only be allowed to access the information.

Due to the lack of the appropriate security technique, information security has become a huge issue. The image encryption mechanism should defined such that the encrypted image will only converted back to the plain image at receiver end by authorized personnel with key [2]. Also, the reconstructed image must be lossless. Pixel correlation is the relation of the pixel to its surrounding pixel values that needs to be addressed while defining the encryption function. Other various encryption engines which assure very virtuous encryption approach for encrypting multimedia. Most of them are known namely RSA [3], DES [4] etc. They encrypting textual data but as far as the image encryption is concerned it uses more space and take more time because of bulk image data (pixel values) in all the three layers. It should be noted that these encryption and decryption operations are guided by some specific keys, where the keys may be same or can be easily derived from the knowledge. Such cryptographic techniques are grouped under private key cryptography [5], [6]. Alternately, encryption and decryption keys may be different or it may not be feasible to derive one key even though the knowledge of other key is available, and such cryptographic methods are known as public key cryptography [4].

A well-defined encryption should not only minimize the correlation between the pixels but also fast enough to execute quickly while encrypting data. In addition, the good encryption scheme should provide both privacy and security and is lossless in nature. It should be tough enough to have immunity against cryptanalysis and possesses a multi objective problem minimizing the correlation impact among the pixels. So it is important to reduce the correlation between the surrounding pixels and increase the degree of randomness of the image. But it cannot stop an insider (employee, physician, vendor, business partner, etc.) to access the confidential information.

Modern encryption engines are enhanced by various modern approaches however there are some approaches which inherently have different characteristics and hence conflicting relation held among them. In this paper, we propose a novel algorithm that helps in reducing the correlation among the pixel by using switching-gray code mechanisms which will further enhance the security of the cover image. The proposed method considers the whole image as one to work upon, we slice the image into various slices horizontally and vertically and shifting them which will further reduces correlation and hence increase encryption index. In addition, we implement a simple switching methodology to enhance the crypto benefits against cryptanalysis techniques. The technique is implemented on the existing Fibonacci Bit Plane Decomposition Algorithm [2] and the results are found to be improved. Moreover, there are no alterations on the total size of image during encryption and decryption process.

doi : 10.17950/ijset/v5s6/605

The rest of this paper is organized in following manner. In Section 2, we introduce the existing Fibonacci based decomposition and propose a novel method which will work upon the existing one. Section 3 introduces the new approach formula where the modern gray code switching algorithm has been implemented. Section 4 deals with proposed system framework and the basic steps used. Section 5, includes the simulations results associated with proposed algorithm. The conclusion of the paper is presented in the section 6.

BACKGROUND

In this section, a detail survey on existing digital image manipulation algorithms that are readily available for digital encryption is presented. It is very simple to tamper with any image and make it available to others by presenting ownership, authentication proof. Thus fore, insuring digital media integrity has therefore become a major concern among the researchers in the current digital era. Encryption is one of the most common techniques for incorporated by organizations as tool for integrity enforcement, secured communication, tampered proof channel and authentication. In this paper, we present a novel image encryption method which initially rearranges the image on the basis of switching gray codes and pixel explosion then carries out existing encryption algorithms. Compared to the techniques and protocols for security usually employed to perform this task, a particular emphasis on correlation between the neighbor-hood pixels.

Some efficient ways are suggested by Chaos based cryptographic algorithms to develop secure image encryption techniques. An image encryption based on hyper-chaotic map meets the requirements of the secure image transfer. The ergodic matrix of one hyper-chaotic sequence is used to permute image, the form of which is decided by a chaotic logistic map, the other hyper-chaotic sequence is used to diffuse permuted image. To make the cipher more robust against any attack, we have to process several rounds of permutation and diffusion. The initial conditions of the hyper-chaotic map are modified after every round. The results of various experimental, statistical analysis and key sensitivity tests proves that the proposed image encryption scheme provides an efficient, effective and secure way for image encryption and transmission [7].

M- Sequence based on Image scrambling parameter can be produced by a series of shift registers is introduced as pseudo encryption algorithm. In addition, the parametric M-sequence is exploited wherein; the user can change the security keys, r, which indicates the number of implemented shift operations , or the distance parameter p, to generate many different M-sequences. Thus ensuring the scrambled images are difficult to decode while offering a high level of security protection for the images. The algorithm presented here can encrypt the 2-D or 3-D images in one step. It also algorithms immune against the image attacks such as data loss and noise attacks [8]. The algorithm can be applied in the real-time applications as it is a straightforward process and can be easily implemented.

Image encryption is an effective method to protect images or videos by converting and transferring them into unrecognizable formats for different security purposes. To improve the security level of encryption approaches based on bit-plane decomposition, a new image encryption algorithm by using a combination of parametric bit-plane decomposition along with shuffling and resizing, pixel scrambling and data mapping. The algorithm incorporates the Fibonacci P-code for image bit-plane decomposition and the 2D P-Fibonacci transform for image encryption because they depends on parameter. In addition, shuffling the order of the bit-planes enhances the cryptographic benefits of the framework. Simulation analysis and comparisons prove that the algorithm's performance against existing image encryption is considerable effective while immune against several common attacks [9].

Further, a new parametric n-array Gray code, the (n, k, p)-Gray code, which includes several commonly used codes such as the binary-reflected, ternary, and (n, k) - Gray codes. The new (n, k, p) - Gray code has potential applications in digital communications and signal/image processing systems with focus on three illustrative applications of the (n, k, p)-Gray code, namely, image bit-plane decomposition, image de- noising, and encryption are demonstrated. The computer simulations prove that the (n, k, p)-Gray code offer better performance than other traditional Gray codes for these applications in image systems [10].

A detail subfamily of the generalized Fibonacci sequence family termed as distinguished generalized Fibonacci sequence are introduced [11]. Prime focus was on two members of this subfamily, the Fibonacci sequence and the Lucas sequence and two transformations, based on these sequences, are illustrated in detail. The applications of these transformations to image scrambling are found to have the desirable property of uniformity, that is, after scrambling the pixels that are equidistant in the original image remain equidistant, albeit with different distance values. The adjacent pixel spreads as far as possible by these transforms. The properties and periodicity of the 2-D Fibonacci transformation of digital images are discussed and a new computation method [12] and an accurate formula are also given. A new digital image scrambling method based on Fibonacci numbers is introduced based on the uniformity and periodicity of the scrambling transformation [13]. The scrambling transformation employed is expressed to have the following advantages: (1) encoding and decoding is very easy and can be applied in real-time situations (2) the scrambling effect is very good, the information of the image is re-distributed across the whole image randomly; and (3) the method can endure common image attacks, such as compression, noise and loss of data packet.

An image encryption method based on the Generalized P-Gray Code (GPGC) which is a parametric sequence and suitable for any base (n) to protect multimedia information for different security purposes is illustrated [14]. New image bit-plane decomposition is incorporated based on GPGC to develop two image encryption algorithms. The two algorithms allows for either full or partial encryption of images based on the choice of security keys: distance parameter p and base n. Experimental results prove that the presented algorithms are lossless encryption methods, and when the correct keys are used, the original images can be completely reconstructed. It can also withstand the plaintext attacks.

PIXEL EXPLOSION AND SWITCHING TECHNIQUES

In an ideal encryption algorithm, the correlation between the two diagonally adjacent, vertically adjacent and horizontally adjacent pixels of the ciphered image should be low. Further, this method could be proven to be very strong in combination with the weaker and less secure encryption techniques. In brief, the image is viewed as the combination of the pixels (RGB layers) which is the smallest element of an image that contains the image characteristic in an isolated form. These RGB pixel values in general, have high correlation with the neighboring pixels due to the gradual change in the image characteristics.

Pixel explosion is a technique that focuses on shifting out of the native pixel and shifted into some other pixel in lying within the image boundaries. Thus, the correlation between the pixels in given layer could be minimized drastically. In this paper, the shift employed and discussed are linear and circular. The circular shift ensures that there is no loss of data or overwriting of the values. The Shifting of the values are based on certain rules and inferences from the key provided at the beginning of the process. This key is essential for successful reconstruction of the cover image from its cipher and provides crypto benefits against brute force attack.

R. J. Mathews et.al [15] introduced an image encryption which focuses on complete breakdown of digital image into its RGB components and then performing the shifting and permutations on these elements based on a key. The shade of entire encrypted image changes by the inter-pixel shifting of R G B values. Figure 1, illustrates the pixel explosion techniques that are incorporated to generate ciphered image from a plain cover image.

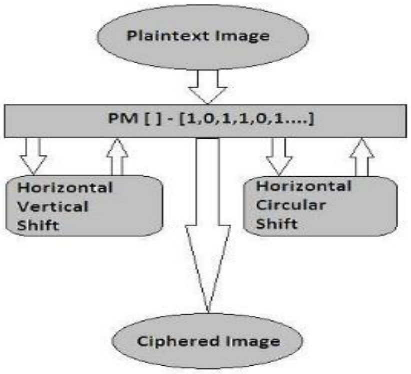
Plaintext Image
PM [ ] - [1,0,1,1,0,1....]
Horizontal Vertical Shift
Horizontal Circular Shift
Ciphered Image

Fig 1. Pixel Explosion Scheme [15]

Switching theory is a well-known technique employed in designing intelligent controllers for logic controls. Its applications extend to various fields of engineering, bio-technology, marketing and etc. The distribution of the pixels varies from one region to another and from one neighborhood to another within a given region. Existing methods treat every pixel (expect zero) within a block with the same manipulation technique. Hence, we incorporated the well switching theory into the proposed algorithm for capitalizing this issue and enhance the crypto efficiency and simultaneously enhance its immunity against brute-force attack. The simplest block diagram for switching mechanism is presented in the figure 2.

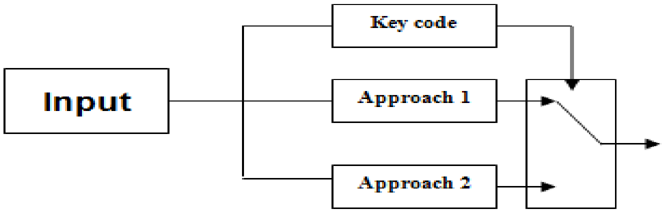

Fig 2. The basic structure of the Switching Mechanism incorporated

The input is data that has varying characteristics (such frequency, redundancy components or etc). Key-code is parameter that is user defined which acts as basis for switching between two approaches. Approach 1 is a mechanism that is need to performed under certain constraints and approach 2 is another that is performed in the remaining.

PROPOSED ALGORITHM

To design a secured encryption scheme, it is not only vital to know how to manipulate/alter data within a cover image but also we need to know how to reconstruct the original information from manipulated/altered data of the cover image. In this section, we present in detail the features of the proposed encryption algorithm for digital images based on pixel explosion and switching gray-code encoding. In addition, we also explain about correlation based relationship between the image sub-blocks and manipulate data bit for successful reconstruction of encoded data. The proposed algorithm could effectively reconstruct the encrypted information lossless with authorized knowledge of the keys associated during the encryption of original cover media. The Fig.3 presents a detail block diagram of encoding and decoding process of the proposed algorithm.

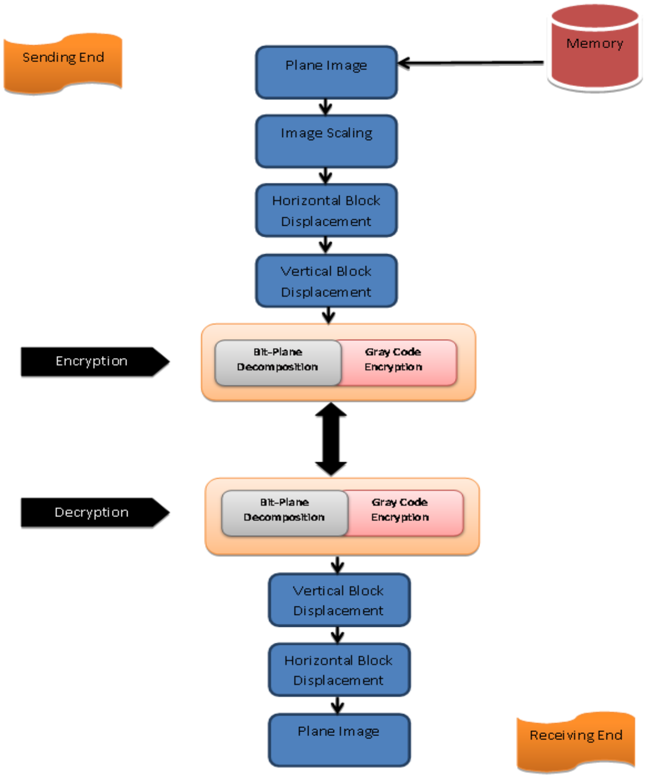

Fig 3. Block Diagram of Encoding and Decoding Process of the proposed algorithm

In the block diagram presented in the figure 3, the vertical &horizontal block displacement plays a significant role in pixel explosion of either column-wise (or) row-wise manipulation process that would help in minimizing the correlation effect within the cover image. Direct encoding as discussed in prior section results in maintaining the correlation factor on similar lines (i.e. before and after encryption) which might not be feasible in modern encryption techniques. Therefore the proposed encryption approach encrypts data in a manner that it could not be retrieved without the authorized knowledge keys incorporated for encryption process. We enforce a specific relation based on which the pixel explosion is carried out using switching mechanism wherein key based pixels are altered using gray-code mechanism while other pixels would remain unaltered thus boasting the crypto benefits. In addition, the secured data encrypted using the proposed scheme maintains the visible artifacts while maximizes the distortion and limit the changes to highly correlated areas.

A. *Encoding Process*

Input: The secured data which is to be encrypted
Step1: Choose the key-code for pixel explosion
Step2: Decompose the cover image into various rows. And differentiate rows into unchanged and gray-code based switching and key-code.
Step3: Decompose the cover image into various columns. And differentiate columns into unchanged and gray-code based switching and key-code. ***Step4:*** Convert the encrypted data into a binary stream of the bits Convert the each bit into gray-code, and append to encrypt stream
Step5: Recombine the encrypted stream into image blocks based on the key
Step6: Determine the encryption that could be incorporated over the uncorrelated bits encryption algorithm
Output: Crypto image with secured digital keys

The main focus of any encryption system is to attain a high un-correlation among the neighborhood pixels while maximizing the visible or statistical distortions in the cover image. Hence, we could shuffle data randomly before manipulating the data based on key that could transferred with the image or externally.

B. *Decoding Algorithm*

The decoding system is quite simple and the exact reserve procedure of the encoding process. The general steps in reconstruction the cover data from encrypted information are:

Input: Input the Crypto image and digital key.
Step1: Decompose the crypto image into various binary stream based on the key.
Step2: Convert gray-code of bit to corresponding binary code Convert the bit into digital image,
Step3: Recompose the cover image through various columns after differentiates columns into unchanged and gray-code based switching and key-code.
Step4: Recompose the cover image through various rows after differentiates rows into unchanged and gray-code based switching and key-code.
Step5: Recombine the reconstructed binary information

Output: Output the reconstructed cover image.

The reconstructed cover image has no distortion from the original cover image. We could enhance the integrity of the system by switching gray-code and pixel explosion techniques as the encryption pre-process. Various researchers are developing/proposing frameworks that could help better analyzing the media in consideration which would enhance the robustness of the secured systems. In addition, the proposed system exploits signal analysis such as, localized information (i.e. correlation factor) in time domain that is in the demand for the real field defined encryption frameworks.

COMPUTER SIMULATIONS AND RESULTS

In this section, the simulations results of proposed switching gray-code and pixel explosion based encryption system for digital images are presented in detail. Computer simulations were simulated using MATLAB software package. Analysis was done using various color and gray-scale bitmap images varying in size, type, and classes of image features. These images were stored as uncompressed TIFF some of which are later converted into bitmap images by threshold.

Visual Analysis Test: In this test, we check the feasibility of the proposed system and visual distortion of the proposed system at each stage of the operation. The figure 4 , presents the original "Airbus" cover image and every output image after each stage i.e. .Horizontally Shifted using 1:2:3 rule + gray code encryption, Vertically Shifted using 1:2:3 rule + gray code encryption, Gray Code encryption of global image, Fibonacci Bit place decomposition algorithm.

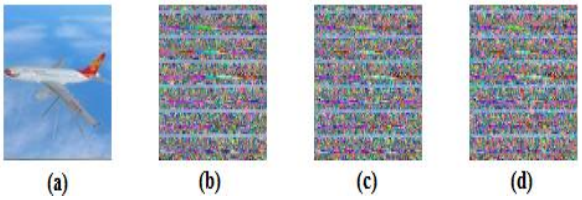

Fig.4 a) cover image "Airbus", b) partially encrypted image "Horizontal + gray-code encrypted", c) partially encrypted image "Vertical + gray-code encrypted", d) encrypted image

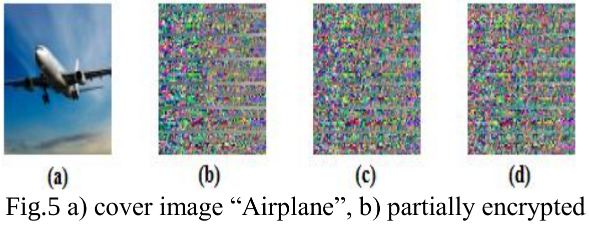

Fig.5 a) cover image "Airplane", b) partially encrypted image "Horizontal+ gray-code encrypted", c) partially encrypted image "Vertical + gray-code encrypted", d) encrypted image

The figure 5, presents the original "Airplane" cover image and every output image after each stage i.e. Horizontally Shifted using 1:2:3 rule + gray code encryption, Vertically Shifted using 1:2:3 rule + gray code encryption, Gray Code encryption of global image, Fibonacci Bit place decomposition algorithm. The figure 6 , presents the original “Flower” cover image and every output image after each stage i.e. Horizontally Shifted using 1:2:3 rule + gray code encryption, Vertically Shifted using 1:2:3 rule + gray code encryption, Gray Code encryption of global image, Fibonacci Bit place decomposition algorithm.

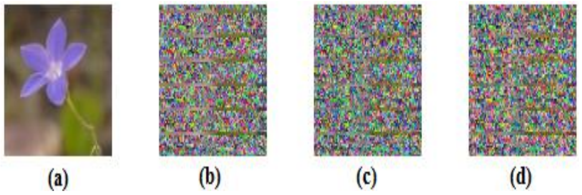

Fig.6 a) cover image “Flower”, b) partially encrypted image “Horizontal+ gray-code encrypted”, c) partially encrypted image “Vertical + gray-code encrypted”, d) encrypted image

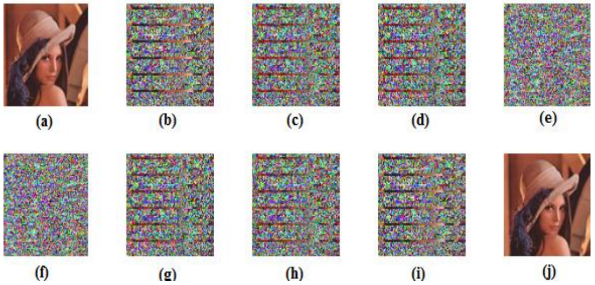

Fig.7 a) cover image “Flower”, b) partially encrypted image “Horizontal+ gray-code encrypted”, c) partially encrypted image “Vertical + gray-code encrypted”, d) encrypted image (gray-code shifting) e) encrypted image after Fibonacci f) Fibonacci encrypted image g) decrypted image (gray-code shifting) h)decrypted image “Vertical + gray-code decrypted”, i) decrypted image “Horizontal + gray-code decrypted” and j) decrypted cover image

The figure 7 , presents the complete process of encoding and decoding of the original “Lena” cover image and every output image after each stage of the encoding process [figure 7, a-e] and every output image after each stage of the decoding process [figure 7, f-j]. It is evident from this test that the visible artifacts are preserved with reference to the cover image to decrypted image. In addition, the proposed approach is lossless in nature i.e. there is no change in decrypted image from original cover image. Further, the proposed approach is effective for real-time applications and simple to use.

<u>First-Order Analysis Test</u>: In this test, we check the first-order statistics of the cover and encrypted image to estimate the possible combinations to break the code via brute-force attack. The figure, presents the comparison between the original cover to encrypted image to decrypted image. It is evident from this test that the first-order statistics are preserved with reference to the cover image to decrypted image. In addition, the proposed approach is immune to brute-force quite significantly i.e. it is hard to decrypt the encrypted image without prior knowledge of the keys incorporated.

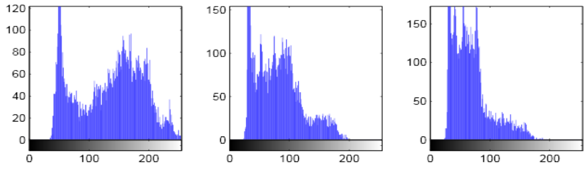

Fig.8 The histograms of red-green-blue layers of the original cover image “Lena”

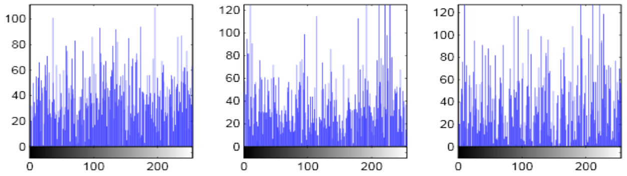

Fig.9The histograms of red-green-blue layers of the encrypted image “Lena” after the encoding proposed algorithm

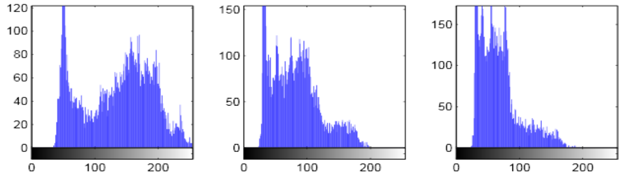

Fig.10 The histograms of red-green-blue layers of the decrypted image “Lena” after the decoding proposed algorithm

<u>Statistical Analysis Test</u>: In this test, we compare between various inherent image features like “RMS”, “PSNR”, “correlation factor” which shows the feasibility of the proposed algorithm to various types of encryption algorithms as illustrated in table 1, table 2 & table 3. And corresponding figures are presented in figure 11 and 12.

PERCENTAGE PIXEL CHANGE IN EACH LAYER OF ‘LENA.BMP’

Shift Code	Fibonacci Bit Plane Decomposition Algorithm			Proposed Algorithm		
	R	G	B	R	G	B
1	50.866	68.5615	65.5436	33.26	33.26	32.41
2	69.1407	75.3127	68.5037	33.26	33.26	32.59
3	83.5613	89.4482	72.4209	33.17	33.27	32.48
4	86.4494	88.8537	75.8502	32.58	33.20	33.21
5	79.7377	83.8537	81.6119	33.17	33.20	33.21
6	71.5777	79.0445	87.9407	33.23	33.17	33.23
7	59.9112	75.0346	81.5545	33.24	33.18	33.24
8	58.5200	77.0777	79.0613	33.24	33.20	33.25
9	59.1331	77.8064	76.6423	33.23	33.20	33.20
10	64.8669	83.3201	79.3222	33.17	33.20	33.15
11	75.6144	87.6402	84.9092	33.20	33.20	33.24

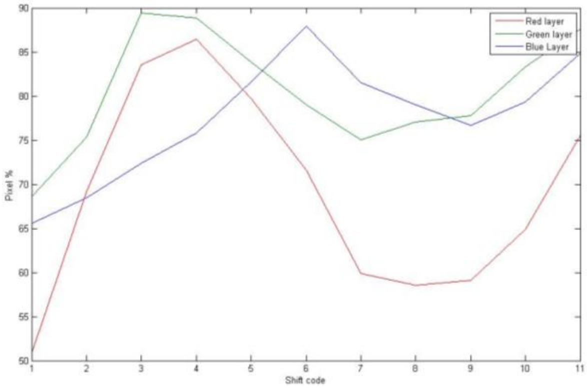

Fig.11 The pixel % change of red-green-blue layers of the encrypted image "Lena" after the encryption algorithm

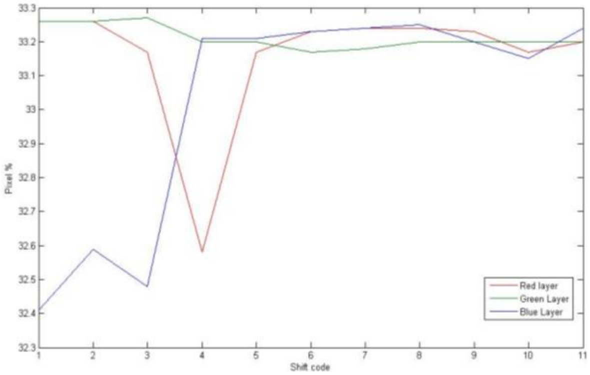

Fig.12 The pixel % change of red-green-blue layers of the encrypted image "Lena" after the proposed encryption algorithm

Percentage pixel change

Images	Percentage Change
'Lena.bmp'	99.64
'Airbus.jpg'	99.64
'Airplane.jpg'	99.59
'Flower.jpg'	99.57
'Flower1.png'	98.93

Correlation Between Pixel

Images	Original	Encrypted
'Lena.bmp'	0.0936	0.0868
'Airbus.jpg'	0.1420	0.0889
'Airplane.jpg'	0.0987	0.0906
'Flower.jpg'	0.0993	0.0868
'Flower1.png'	0.4144	0.4112

In the above test we have recognized that the proposed system could provide effective encryption in comparison with the existing algorithm. The table I to table III shows data shows pixel change for each layer for some of the shift code for various images. In addition the correlation is reduced to min value of 0.0889 for "airbus.jpg" which shows maximum distortion between the cover and cipher image. Furthermore, the attacker may use the brute force attack that tries all possible combination to construct the perfect master image.

Conclusion

In this paper, we introduced a novel image encryption method which initially rearranges the image on the basis of switching gray codes and pixel explosion. The simulation results show that switching gray-code and pixel explosion significantly reduces the correlation impact within the neighborhood while encrypting the cover image. It is evident that this framework could be employed for partial encryption in real-time applications and videos. The pixel explosion uses well-defined key that switches between the gray-code of the image pixels. Thus, the proposed algorithm enhances security of the cover information. Further, experimental results shows that the proposed pixel explosion is enough for partial encryption and enhances security of the data. In addition, it could also support as an armament for any existing algorithm.

References

i. *Goel, A., & Chandra, N. (2012, May). A Technique for Image Encryption Based on Explosive n* n Block Displacement Followed by Inter-pixel Displacement of RGB Attribute of a Pixel. In Communication Systems and Network Technologies (CSNT), 2012 International Conference on (pp. 884-888). IEEE.*

ii. *C. C. Ravindranath, Bhatt A K and Bhatt A; "Adaptive Cryptosystem for Digital Images using Fibonacci Bit- Plane Decomposition" International Journal of Computer Applications (0975 – 8887)Volume 65– No.14, March 2013*

iii. *RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-2-6.html*

iv. *DES. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. The urlexplains the concept of the Data Encryption Standard.*

v. *S. S. Maniccam and N. G. Bourbakis,"Image and video encryption using scan patterns," Pattern Recognition 37, pp. 725-737, 2004. NJ: Prentice Hall, 2003.*

vi. *B. Furht, D. Socek, and A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," Chapter in Multimedia Security Handbook, pp. 94 – 144, CRC Press, 2005*

vii. *L. C. L. Chuanmu and H. L. H. Lianxi, "A New Image Encryption Scheme based on Hyperchaotic Sequences," 2007 Int. Work. Anti-Counterfeiting, Secur. Identif., 2007.*

viii. *Y. Zhou, K. Panetta, and S. Agaian, "An image scrambling algorithm using parameter based M-sequences," in Proceedings of the 7th International Conference on Machine Learning and Cybernetics, ICMLC, 2008, vol. 7, pp. 3695–3698.*

ix. *Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition," Opt. Commun., vol. 285, pp. 594–608, 2012.*

x. *Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-Gray code for image systems," IEEE Trans. Cybern., vol. 43, pp. 515–529, 2013.*

xi. *J. Z. J. Zou, R. K. Ward, and D. Q. D. Qi, "The generalized Fibonacci transformations and application to image scrambling," 2004 IEEE Int. Conf. Acoust. Speech, Signal Process., vol. 3, 2004.*

xii. *W. Zou, J. Huang, and C. Zhou, "Digital image scrambling technology based on two dimension fibonacci transformation and its periodicity," in Proceedings - 3rd International Symposium on Information Science and Engineering, ISISE 2010, 2011, pp. 415–418.*

xiii. *J. Z. J. Zou, R. K. Ward, and D. Q. D. Qi, "A new digital image scrambling method based on Fibonacci numbers," 2004 IEEE Int. Symp. Circuits Syst. (IEEE Cat. No.04CH37512), vol. 3, 2004.*

xiv. *Y. Zhou, K. Panetta, and S. Agaian, "Image encryption algorithms based on generalized P-Gray Code bit plane decomposition," in Conference Record - Asilomar Conference on Signals, Systems and Computers, 2009, pp. 400–404.*

xv. *Mathews, R., Goel, A., Saxena, P., & Mishra, V. P. (2011, October). Image encryption based on explosive inter-pixel displacement of the RGB attributes of a pixel. In Proceedings of the World Congress on Engineering and Computer Science (Vol. 1, pp. 41-44).*