ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

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

Aditi Malviya [1], Ranjal Agrawal[2], Prof. Rishi sharma[3]

M. Tech Scholar, Dept. of E.C., OIST, Bhopal, Madhya Pradesh, India [1]

B. E Scholar, Dept. of E.C., OIST, Bhopal, Madhya Pradesh, India[2]

Assistant Professor, Dept. of E.C., OIST, Bhopal, Madhya Pradesh, India[3]

ABSTRACT: Now 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.

KEYWORDS: Encryption, Gray-Code, Pixel Displacement

I. INTRODUCTION

In last 2 decades, the uses of computer and networks have grown hugely. As computers and networks are interconnected and installed to form a global network. Huge volume of data is transmitted over the network. So information security is an essential part of communication means everyone wants security of data which is to be transmitted. In recent years the advancement in computer and communications, has allowed potential market to distribute information through the Internet. E-commerce websites have created enormous demand of information security [1]. Ensuring individual has posed increasingly challenging difficulty. The security of digital images has become most important due to rapid and fast growth of internet. Now days the multimedia technology promoted digital images to play a major role which demands security of user's data. For example, the images are widely used in public marketing and advertisements. In defence, the confidential data obtained from military satellite images are to be protected. In medical applications, the transmission of medical image is secured which help to maintain the confidentiality of information about the patients. The image security needs the following characteristics namely [7]:

1. The encryption system should be computationally secure. It needs a tremendously long time to attack an unauthorized user must not be able to read the privileged image.

2. Encryption and decryption should be fast enough. The algorithm for encryption and decryption should be simple sufficient to be used in a personal computer.

3. The security mechanism must be easy going and as widespread as possible.

In wired and wireless networks the major challenge is to protect the confidentiality of images s. To fulfil the requirement of security and privacy, cryptography is used. The information security has two main aspects: confidentiality and authenticity. With fast growth in digital communication, sharing and transmission of images over the Internet is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

unsecured. There are so many cryptography algorithms which are used to provide data communication to be secured by preventing cipher attacks. The significance of image encryption is:

1. Generally, the image data has higher redundancy and bulk capacity which makes encrypted image data vulnerable and this is the primary reason due to which a cryptanalysis attacks the data. From the bulk capacity, anyone can gain enough cipher text samples to the statistical analysis. The data in images have higher redundancy, adjacent pixels likely have similar gray scale values, or image blocks which could have similar patterns and usually embed the image with certain patterns that result in information leakage.

2. The real-time encryption is very difficult, since image data capacity would sufficiently large. In addition to this, a real-time processing constraint is often required for imaging applications, like image surveillance, video conferencing and so on. Bulk amount of image and multi- media data could creates stress not only on the encoding and decoding processes, also the encryption process .Even if an encryption algorithm runs too slowly, with high security features, it would have very little practical value for real-time imaging applications.

3. The image pixels have strong correlations among adjacent pixels and it is very difficult to do fast data-shuffling. The statistical analysis performed on large numbers of image has been that on an average their adjacent (typical values 8 to 16) pixels are correlative in the vertical, horizontal and diagonal directions for both natural and computer-generated images. According to Shannon's (1949) information theory, a secure encryption technique should satisfy the condition on the information entropy, E (P/C) where P stands for plain message and C for ciphered message; i.e., the ciphered image should not contain any information about the plain image [2]. To fulfill this requirement, the ciphered image should be presented in a random manner.

4. In normal usage of image data, file format conversion is a very frequent operation. It is mandatory that image encryption would not affect such operation. Thus, directly treating image data as ordinary data for encryption would make file format conversion impossible. Leaving file header and control information unencrypted is preferred to the image data which is to be encrypted.

II. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

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].

III. 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.

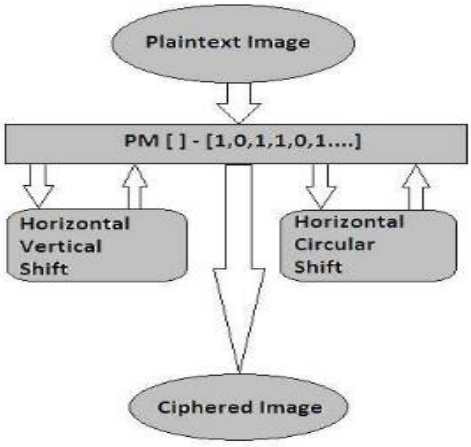

Fig 1. Pixel Explosion Scheme [15]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

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.

IV.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.

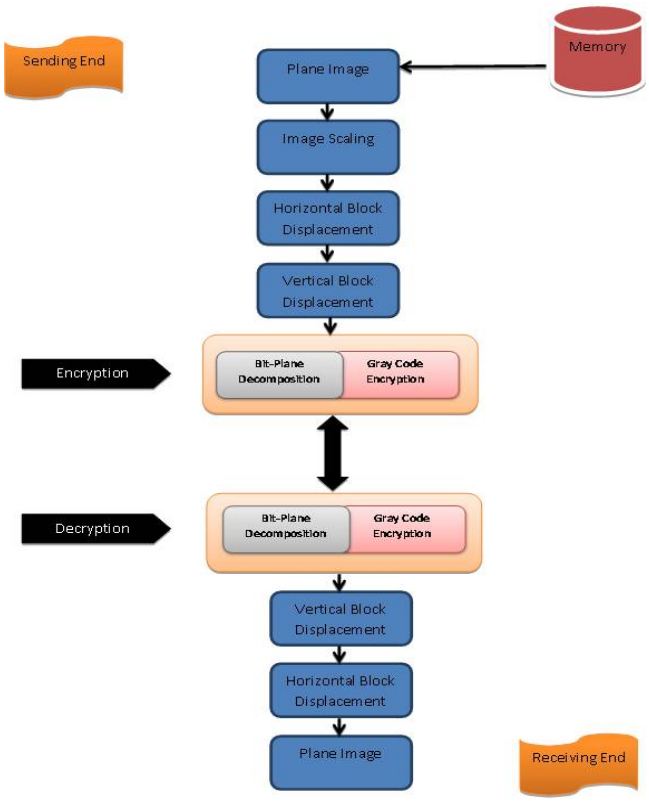

Fig 2. Block Diagram of Encoding and Decoding Process of the proposed algorithm

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

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.

V.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.

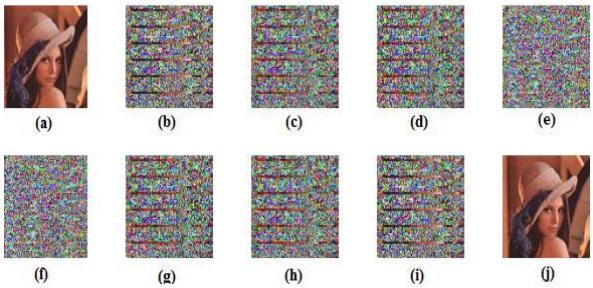

Fig.3 a) cover image "Flower", b) partially encrypted image "Horizontal+ gray-code encrypted", c) partially encrypted image "Vertical + gray-code encrypted", d) encrypted image (gray-code shifting) e) encrypted image after Fibonacci f) Fibonacci encrypted image g) decrypted image (gray-code shifting) h)decrypted image "Vertical + gray-code decrypted", i) decrypted image "Horizontal + gray-code decrypted" and j) decrypted cover image

The figure 3 , 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 4, a-e] and every output image after each stage of the decoding process [figure 4, f-j]. It is evident from this test that the visible artifacts are preserved with reference to the cover

TABLE I. CORRELATION BETWEEN PIXEL

Images	Original Image	Encrypted Image
'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 shows data shows pixel change for each layer for some of the shift code for various

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

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.

VI.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

[1] Goel, A Xianye Li Xiangfeng Meng Xiulun YangYongkai Yin. (2016, May). Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling Volume 8, Number 4, August 2016.
[2] 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
[3] RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-2-6.html
[4] DES. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. The urlexplains the concept of the Data Encryption Standard.
[5] 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.
[6] B. Furht, D. Socek, and A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," Chapter in Multimedia Security Handbook, pp. 94 – 144, CRC Press, 2005
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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).