International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-3, May-2015

IMAGE ENCRYPTION USING HILBERT SPACE FILLING CURVE AND HENON MAP

Kavya K.S , Mrs. Prabavathi

Abstract - A proficient but a simple selective image encryption method is suggested based on Hilbert space filling curve, Region of interest, non-linear chaotic map. The main essence of the suggested scheme is to change the pixel positions of an image via Hilbert space filling curve in a way that it cannot be accessed by unauthorized persons followed by choosing significant region via Region of interest method. Next diffusion process is carried out on the selected significant region by a secret image key procured from non-linear chaotic map. At last, a suitable decryption method is suggested to form original image from the encrypted image. Analysis and experimental results indicates that the suggested method can succeed many goal of selective encryption and is reckoning safe.

Index terms – Region of interest, Selective encryption, Space filling curve,

I. INTRODUCTION

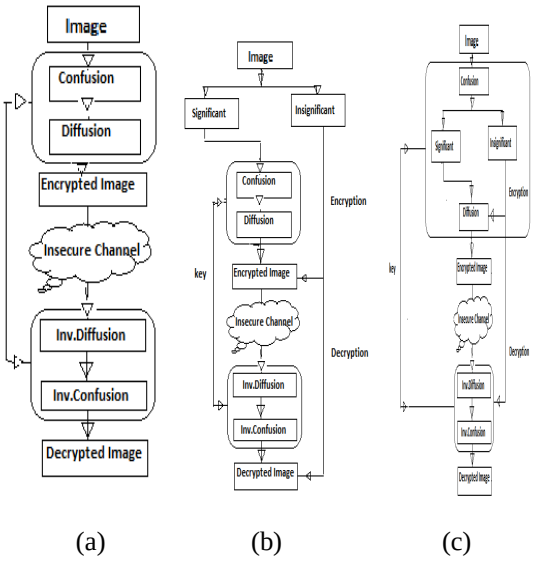
With the enrich in the field of communication and network technology, the different media to convey information via interconnected system and storage on web servers have become important part of it. Though, this amenity causes significantly great decrease in multimedia security. There are so many prospects in multimedia security which consist authentication, copyright protection, confidentiality and access control. Usually, the most important is copy right protection is solved using digital watermarking which encapsulate a mark, called watermark, into the original multimedia and extracts whenever the authorized person needed .contrarily, access control and content confidentiality are solved by encryption process.

Manuscript received May 24, 2015.
Kavya. K. S, P.G. Student, VLSI Design and Embedded System, B.G.S Institute of Technology, B.G.Nagar , Mandya-571448, Karnataka, India. (e-mail: kavyaks37@gmaill.com).
Mrs.Prabavathi, Assistant Professor, Department of Electronics and Communication Engineering, B.G.S.Institute of Technology, B.G.Nagar , Mandya-571448, Karnataka, India.

Encryption is the defined as the process of encoding a multimedia so that it can be read only by the licensed persons. The outcome of this process is called enciphered data. Decryption/ decoding is illustrated as attaining the authentic data from encrypted data and the fusion of these is called encryption techniques. Many encryption techniques have been suggested and used like IDEA, these are frequently used for text data. Hence these techniques are not convenient to accomplish directly on multimedia. Since the multimedia data requires assassinating in its wholeness before users can reach any perception and has high superfluity. So unique encryption techniques are crucial to develop with the regard of structural and statistical properties of multimedia substance . Thus, the prevailing task concentrates on be shield the confidentiality and achieving access preeminence of images. The images are selected for all the preceding sensors like MMW, optical cameras gives the familiarity in the form of images.

There are two approaches in image transmission relying on if encryption should be done on compressed or uncompressed domain. If compression is done after encrypting the image the structural & statistical features of initial image can be changed notably, which gives in lower compressibility. Vice versa if first compression is applied to an image it lowers the calculation overhead however it will damage the syntax of the encoded bit stream and results in reduced secrecy. To come out of this problem selective encryption is introduced here only a part of the multimedia data is encrypted. Hence it can be applied to actual time applications. Here we are concentrating only on partial encryption in uncompressed domain since it gives confidentiality.

The main intention of selective encryption technique is to classify significant & insignificant regions from the image, and later the significant data is encrypted since a small difference in significant part will cause significantly great change in the image. On the other hand, change in the insignificant part will not cause much effect on the image. Hence only significant part of the required data is encrypted additionally it reduces the computational overhead. Below figure shows the difference between partial encryption and conventional methods



(a) (b) (c)

Fig 1.Difference between conventional and selective encryption.(a)conventional, (b)selective encryption scenario I, (c)selective encryption scenario II.

Basically, encryption is split into two sequences i.e. disordering the image (confusion) and encrypting the confused image (diffusion). Confusion diffuses the image elements into muddle by exchanging pixel positions such that the initial image is unrecognizable. Initial image can be recovered back by reverse procedure. Therefore to enhance security and complications confused image will pass through second sequence. In this phase, pixel values changes in such a way that the strong relationship among the pixels will break and this process is called diffusion. Confusion process is solved by so many reversible techniques which is dependent on chaos system, magic square transform, gray code etc..In diffusion process, the image which is confused is transited through the cryptography algorithms like chaos based methods, SCAN based methods etc...there are two model for selective encryption based on the arrangement of pixels which are shown in fig 1(b),(c).in fig.1(b) scrambling the image is local it means confusion is applied to the significant part. On the other hand, in fig 1(c), confusion is applied to the entire image i, e globally. Hence it can be more modified compared to the first model.

II IDEA BEHIND THE PROPOSED WORK

In this paper, a new selective image encryption method is executed in an un-compressed domain which is based on Hilbert SFC, Region of interest (ROI).In the first phase, entire image is scrambled by Hilbert SFC then the significant and insignificant parts of the image is characterized by ROI method. In the second phase, significant part of the scrambled image is encrypted. Using the secret key diffusion procedure is completed successfully and ultimately encrypted image is passed to insecure network channel. The salient feature of the suggested partial encryption technique is secret image. For this purpose, the incipient parameters of non-linear chaotic map are stored at each encryption and decryption ends, acted as keys. Experiment are performed in sequence to see the achieving results and robustness of suggested encryption technique

III. METHODOLOGY

In this chapter some of the driving factors in the design of our attempt to partial image encryption are discussed. The suggested technique uses a color/RGB image and provides an encrypted image which can be decrypted later for so many goals. Without loss of generality, assuming *G* represents the initial color image. The suggested technique consists of three phases. In the first phase, the RGB color channels are converted into Secret independent channels (SEC) using reversible integer transform (RIT) .In second phase, each secret color channel is encrypted. For encryption, first each channel pass through confusion of pixels using proposed Hilbert SFC succeed by the characterization of significant region via Region of Interest. Finally, diffusion is performed on the selected significant region via non-linear chaotic map.

A. RGB to SEC conversion:

R, G and B channels of an image are highly relying upon on each other it being fact that for a good encryption technique this relation must be breeched before encryption in order that the roughness of the technique increases. Generally, RGB channels will be changed into independent transforms like YCbCr, HSI etc. however the important disadvantage is the existing independent transforms is imperfect reconstruction. As a result, for precise color change transformation there must be a conversion which maps integer to integer. For this reason and to improve security, RGB channels are first converted into three secret independent channels (SEC channel) using reversible integer transform (RIT) and soon afterward the encryption is done either in all or any of S, E and C channels.

If transform matrix *A* is elementary reversible matrix (ERM) the general linear transform $Y = AX$ is said to be reversible integer transform. Using any upper or lower matrices we can map integers to integers. Here, bottom TERM is used to generate secret channels (SEC) from typical RGB channel. For instance, if A= $\{a_{ij}: a_{ij}=0 \text{ if } i<j\}_{i, j=1, 2, 3}$ is upper TERM then RGB space is transformed into SEC space as

$$\begin{bmatrix} S \\ E \\ C \end{bmatrix} = \left(A \begin{bmatrix} R \\ G \\ B \end{bmatrix} \right)$$

$$\Rightarrow \begin{bmatrix} S \\ E \\ C \end{bmatrix} = \left[\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \right]$$

and the RGB channel is again obtained from SEC channel as

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \left(A^{-1} \begin{bmatrix} S \\ E \\ C \end{bmatrix} \right)$$

$$\Rightarrow \begin{bmatrix} R \\ G \\ B \end{bmatrix} = \left(\begin{bmatrix} \frac{1}{a_{11}} & 0 & 0 \\ -\frac{a_{21}}{a_{22}} & \frac{1}{a_{22}} & 0 \\ -\frac{a_{31}}{a_{33}} & -\frac{a_{32}}{a_{33}} & \frac{1}{a_{33}} \end{bmatrix} \begin{bmatrix} S \\ E \\ C \end{bmatrix} \right)$$

Definition of term indicates that there are integer factors on diagonal that does not change its magnitude, if inputs are in integers then output will be in integers. If the off-diagonal elements of A are all zero then Reversible Integer Transform lowers to each secret color space by a given factor.

B. Encryption process:

Input image to the encryption process is the image to be shield and results the encrypted image whose size is similar as that of input original image. The entire encryption process consist the following steps:

a. The RGB color channels of initial image *G* are first transformed into SEC color channel.

b. Confusion: changing the pixel positions of image via Hilbert SFC .

c. Characterizing significant and in-significant pixels in confused image *Fs* via Region of interest (ROI) method.

d. Select *R*% significant region.

e. By adopting K_0 and μ *a*s the keys, iterate generalized logistic map to generate *v*alues.

f. Diffusion: Change the pixel value of significant region using matrix key to get the encrypted significant region.

g. Map encrypted significant coefficients onto their original positions.

h. SEC color channels are transformed back to RGB color channels to get encrypted image

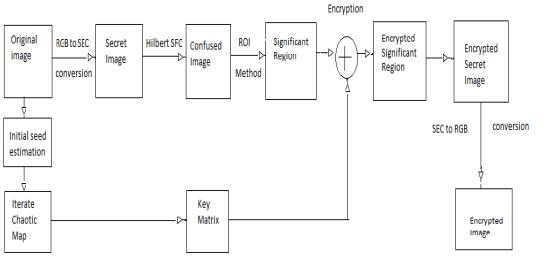


Fig 2.Block diagram of suggested encryption process

C. Decryption Process:

The main goal of the decryption process is to get the image as precisely as feasible from the encrypted image .

a. The RGB color channels of encrypted image are first converted in SEC color channel .

b. Obtain encrypted significant region by selecting *R*% region red based on the saved positions of significant region.

c. By adopting keys K_0 and μ, step 5 to step 10 of encryption process are performed to get matrix key.

d. Inverse diffusion: Obtain the decrypted significant region with the help of matrix key.

e. Map decrypted region to their original positions to get the decrypted confused image.

f. Inverse confusion: Inverse Hilbert SFC is performed .

g. SEC color channels are converted back to RGB color channels to get the decrypted image

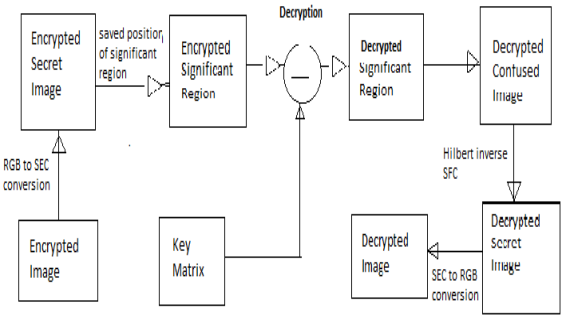


Fig 3. Block diagram of decryption process

IV. EXPERIMENTS AND SECURITY ANALYSIS

Security is the main concern of encryption techniques. An effective encryption technique should be sensible against all type of cryptanalytic and statistical attacks. In this part, a accomplish investigation is made on the security of the suggested encryption technique like sensitive analysis, numeric analysis to demonstrate that the suggested

encryption technique is secure against the most happening attacks.

a. **Key Sensitivity Analysis:** keys play an important role in the security of information system. According to principle, a few changes in the keys never give the precise decryption for good security. For this reason, the key sensitivity of the suggested technique is acceptable. In this technique, three keys (k, μ and $k_{0)}$ are used. Among these, key *k* is an integer of the form 2*b*: *b* > 0. Changing the value of *k* one cannot get the correct decrypted image. Hence, the proposed technique is quite sensitive to *k*. Similarly, the decrypted images with slight change in K_0 and μ will result in non-perfect decryption. Hence, the proposed technique is highly sensitive to the keys.

V RESULT

The accomplishment of the suggested selective encryption technique is demonstrated using MATLAB. So many experiments have done on RGB microcell image, which is used as initial image which have 256*256 sizes.

Figure 4 shows the original microcell image. Figure 5 shows the Secret Independent Channel of microcell image. Fig 6 shows the encrypted image of microcell. Fig 7 shows the decrypted image of microcell. Fig 8 shows the selected region in Secret Independent Channel of microcell image. Fig 9 shows the encrypted image of selected region of microcell. Fig 10 shows the decrypted image of selected region of microcell.

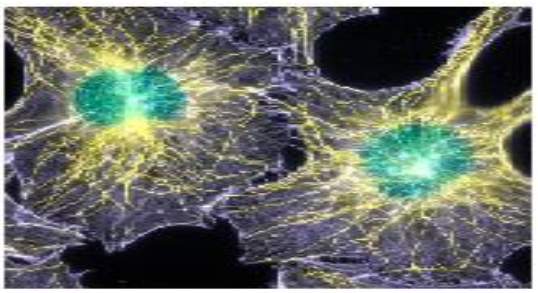


Figure 4 shows the original microcell image

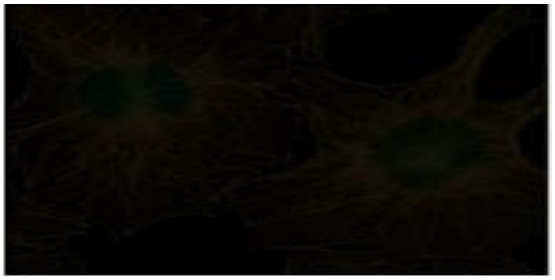


Figure 5 shows the Secret Independent Channel of microcell image

Fig 6 shows the encrypted image of microcell

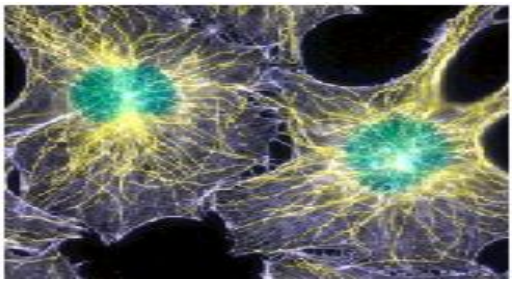


Fig 7 shows the decrypted image of microcell.

Fig 8 shows the selected region in Secret Independent Channel of microcell image

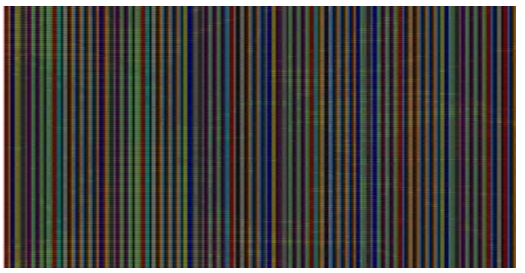


Fig 9 shows the encrypted image of selected region of microcell.

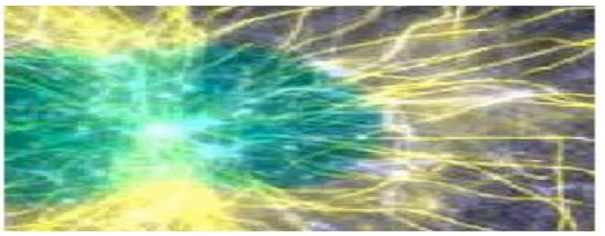


Fig 10 shows the decrypted image of selected region of microcell.

VI. CONCLUSION AND FUTURE WORK

This paper suggests a simple yet efficient partial encryption technique that encrypts a selected image via Hilbert space filling curve, Region of interest, non-linear chaotic map. Hilbert space filling curve is used for scrambling the image. Region of interest is used to characterize the significant and insignificant region , Non-linear chaotic map is used to encrypt the scrambled image. Security analysis is also explained that the right fusion of keys is necessary unveil the initial image. In addition, implied technique has advantage of convenient realization, less computational complexity and a good security .Implied algorithm is opportune for all kind of color image and in future it can be expanded for video also. This extension can be easily done by adopting suggested technique separately to each frame.

REFERENCES

[1] I.J. Cox, M. Miller, J. Bloom, Digital Watermarking, Morgan Kaufmann, San Francisco, 2002.

[2] R.A. Mollin, An Introduction to Cryptography, CRC Press, Boca Raton,FL, USA, 2006.

[3] S. Lian, Multimedia Content Encryption: Techniques and Applications, Taylor & Francis Group, LLC, 2009.

[4] A.M. Alattar, G.I. Al-Regib, S.A. Al-Semari, Improved selective encryption techniques for secure transmission of MPEG video bitstreams, Proceedings – International Conference on Image Processing 4 (1999) 256–260.

[5] H. Cheng, X. Li, Partial encryption of compressed images and videos, IEEE Transactions on Signal Processing 48 (8) (2000) 2439–2451.

Kavya .K .S pursuing 4th semester M.Tech VLSI Design and Embedded System in B.G.S. Institute of Technology, B. G. Nagar, Mandya , Karnataka, India. She Received her B.E (Electricals and Electronics) degree from NIEIT college of Engineering, Mysore in 2013 .She has interest in the field of image processing. She had presented her paper in National conference on Emerging trends in Electronics and Communication (NCETEC-15).