© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

In-Dependable Data hiding in an Encrypted Image using FCM-DH Algorithm

Vinodhkumar L,Vinoth B S, SivaGanesh S
Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

In this paper, a data mining technique, Fuzzy C Means Clustering (FCM) based data hiding algorithm (FCM-DH) is used to divide pixels into classes or clusters from the encrypted image. Clustering of pixels in an encrypted image is considered in the proposed approach for creating a space to accommodate data. Before applying the FCM-DH, a content owner prepares a cover image by encrypting the pixels of an image with encryption key. Then, group the pixels to compress the least significant bits of the encrypted image using a proposed FCM-DH technique with data-hiding key and form a partition matrix to create space to accommodate data. With a received cover image containing hidden data, if the receiver can extract the data with data-hiding key or decrypt the cover image with encryption key to obtain original image independently. If the receiver applying both the data-hiding key and the encryption key, then extract the data and recover the original image without any error by exploiting the spatial correlation in natural image.

Keywords: Image Encryption, In-Dependable Data Hiding, FCM-DH algorithm

I. INTRODUCTION

With the tremendous growth of internet and significant development in multimedia technologies in recent years the transmission of multimedia data such as audio, video and images over the internet is now very common. The Internet, however, is a very insecure channel and this possesses a number of security issues. The security and the confidentiality of sensitive and multimedia data has become of prime and supreme importance and concern.

To protect this data from unauthorized access and tampering various methods for data hiding like cryptography, hashing, authentication have been developed and are in practice today. In recent years, signal processing in the encrypted domain has attracted considerable research interest.

Related Works

While an encrypted binary image compression and the degree to which the data must be immune to interception, modification, or removal by a third party [1], FCM is a method of clustering which allows one piece of data to belong to two or more clusters in [2]. With the Lossless generalized-LSB data embedding method presented in [4], an encrypted gray image can be efficiently analyzed and Security evaluation of image encryption schemes [3], and reversible data embedding using a difference expansion method presented in [5]. Pixels of an encrypted image are compressed by form a partition matrix PMi,j to create a space to accommodate data using the proposed FCM based clustering technique and data can embedded into the image in reversible way, therefore the receiver can extract the data and the image independently with the help of keys.

II. METHODS AND MATERIAL

The proposed methodology is consists of three phases image encryption, data embedding and data-extraction/image-recovery. The content owner encrypts the original image using an encryption key to produce an encrypted image. Then, apply the proposed FCM based data hiding technique to form clusters of pixels and a partition matrix is formed by the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the data.

At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image

containing hidden data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original one. When using both of the encryption and data-hiding keys, the embedded data can be successfully extracted and the original image can be recovered without any loss by exploiting the spatial correlation in natural image.

A. Image Encryption

Assume the original image with a size of *N1 X N2* is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits.

Denote the gray value as $P_{i,j}$, where *i,j* indicates the pixel position, and bits of a pixel as $b_{i,j,0}$, $b_{i,j,1}$,..., $b_{i,j,7.}$ The gray value is converted into bits.

$$b_{i,j,k} = \left\lfloor \frac{P_{i,j}}{2^k} \right\rfloor \bmod 2, \quad k=0,1,\ldots,7$$

8 bit representation of each pixel of an image is encrypted by performing XOR with the $r_{i,j,k}$ which is determined by an encryption key to create a cover image.

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k}$$

B. Data Embedding

In this phase, three parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are randomly permuted and compressed to form a partition matrix $PM_{i,j}$ to create a space for accommodating the data by the proposed FCM-DH algorithm.

Algorithm: FCM-DH

Inputs *CI cover (encrypted) image, $D_{[1,\ldots n]}$ data, and K data-hiding key*
Output *image, containing data.*
Initialize *parameters M,PL and I*
Select *N_p/N pixels from CI* ⟵ *parameters*
op ⟵ *$[N\text{-}N_p]^{p(k)}$*
G ⟵ *[N-Np]/PL*
i ⟵ *1*
Do
for *j=1 to PL*
  for *k=1 to M*
    $LSB_{i,j}$ ⟵ *$B_{j,k}$*
  end
end
$cbits_{i,1..M.PL-I}$ ⟵ *$LSB_{i,1,\ldots,}$ $LSB_{i,M.PL-I}$*
$PM_{i,1\ldots I}$ ⟵ *$LSB_{i,M.PL-I+1}, \ldots\ldots, LSB_{i,M.PL}$*
Repeat *group i to G*
$PM_{i\ldots G,1\ldots I}$ ⟵ *$[asci(D_{[1,\ldots.n]})]/2^k \bmod 2$, k=1,..,7*
op ⟵ *$[N\text{-}N_p]^{\sim p(k)}$*
return *CI containing $D_{[1,\ldots\ldots,n]}$*

C. Data Extraction and Image Recovery

In this phase, consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. Note that because of the random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data.

Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data by the inverse process of FCM-DH technique, but cannot get any information about the original image content. Similarly recover the image with encryption key. When the receiver has both of the keys, can extract the data and recover the original content of a cover image without any error by exploiting the spatial correlation in natural image.

III. RESULTS AND DISCUSSION

The test image Koala.jpg sized 300 x 300 shown in Fig.1 (a) was used as the cover image in the experiment. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig.1 (b). The data can embedded into an encrypted image using FCM-DH algorithm is shown in Fig.1(c). With an encrypted image containing embedded data, we could extract the data using the data-hiding key. If we directly decrypted the encrypted image containing embedded data using the encryption key, the directly decrypted image is given in Fig.1 (d)

Fig. 1(a)

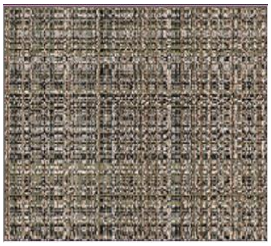

Fig. 1(b)

Fig. 1(a) Original Koala.jpg sized (300 x 300)
Fig. 1(b) Encrypted image

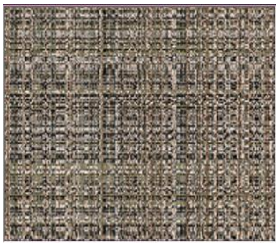

Fig. 1(c)

Fig. 1(d)

Fig. 1(c) Image containing data (result from FCM_DH algorithm)
Fig. 1(d) Directly decrypted image

By using both the data-hiding and the encryption keys, the embedded data could be successfully extracted and the original image could be perfectly recovered from the encrypted image containing embedded data.

IV. CONCLUSION

In this paper, a novel FCM-DH algorithm for in-dependable data hiding in an encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. Therefore the pixels of an encrypted image are compressed by form a partition matrix to create a space to accommodate data. With an encrypted image containing data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the data and recover the original content of an image.

V. REFERENCES

[1] Padmanaban K, Dr. R. JagadeeshKannan, “Localization of Optic Disc using Fuzzy C Means Clustering” IEEE Conference Current Trends in Engineering and Technology, 2013.

[2] W. Bender D. Gruhl N. Morimoto A. Lu, “Techniques for Data Hiding” Ibm Systems Journal, Vol 35, Nos 3&4,

[3] Jawad Ahmad and Fawad Ahmed, “Efficiency Analysis and Security Evaluation of Image Encryption Schemes” International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04.

[4] Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp, Eli Saber, "Lossless generalized-LSB data embedding", IEEE Transaction. on Image Processing, vol.14, No.2, Feb. 2005.

[5] Jun Tian, "Reversible data embedding using a difference expansion", IEEE Trans. on Cirut and sys, vol. 13, No. 8, Aug. 2003.

[6] M. Kiran Kumar, S. Mukthyar Azam, Shaik Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", International Journal of Network Security & its Applications, vol.2, No.4, Oct. 2010.

[7] Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang, "Commutative encryption and watermarking in video compression", IEEE Trans. on Circuits and Systems for Video Technology, vol. 17, No. 6, Jun 2007.

[8] Chinmaya Kumar Nayak, Anuja Kumar Acharya, Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm", International Journal of Research and Reviews in Computer Science, vol. 2, No. 2, Apr. 2011.

[9] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53-58, Feb. 2011.

[10] Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez," A New Chaos Steganography Algorithm for Hiding Multimedia Data" Feb. 19-22, 2012 ICACT 2012.