2013

Image Authentication Using Stochastic Diffusion

AbdulRahman I. Al-Rawi
University of Bahrain, abdulrahman.alrawi@gmail.com

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Recommended Citation

Al-Rawi, A., Blackledge, J.: Image Authentication Using Stochastic Diffusion. System Infomatics: Modelling and Simulation SIMS2013, Cambridge University, 2013, p.1-6.

Image Authentication Using Stochastic Diffusion

AbdulRahman I. Al-Rawi
College of Applied Studies
University of Bahrain
Kingdom of Bahrain
aalrawi@uob.edu.bh

Jonathan M. Blackledge
School of Electrical Engineering Systems
Dublin Institute of Technology
Dublin, Ireland
jonathan.blackledge@dit.ie

***Abstract*—This paper considers an approach to encrypted information hiding based on Stochastic Diffusion for encrypting digital images coupled with the application of a Least Significant Bit (LSB) method for information embedding. After providing a brief summary of various information hiding methods based on spatial and transform domain techniques, two new methods are introduced. The first of these considers a binary image watermarking algorithm for hiding an image in a single host image which is based on binarization of the encrypted data. The second method extends this approach to solving the problem of 24-bit image hiding in three host images which generates a near perfect reconstruction after decryption. Both methods make use of a 'hidden code' technique to randomize the order of the embedded bits and the location (in the image plane) of the LSBs which make the embedded information more robust to attack. Details of the algorithms developed are provided and examples are given, which have application in the field of covert cryptography and the authentication of full colour images for copyright protection and Data Rights Management.**

***Keywords*-Encrypted Information Hiding; Stochastic Diffusion; Hidden Codes.**

I. Introduction

Following rapid developments in computer networks and digital media transmission (e.g. digital image, audio and video data) along with the fast growth of Internet connectivity, the demand for securing data exchange over the Internet has become increasingly important. Transmission of data over networks and Internet-based dissemination of digital information has brought about several security issues. Illegal distribution of digital media, copyright protection of digital data, copying, and unauthorized information interception are common problems requiring innovative and novel solutions. Of these, cryptography remains the most common. There are a large number of commercially available cryptosystems for data encryption that are considered computationally secure and are relatively difficult to break [1]-[9], but using cryptography does not necessarily assure security of a transmission; the meaningless form of data after encryption leads to suspicion of its importance and potential attack. In addition, rapid improvements in the computational performance and sophistication of attack methods threaten the security of encryption techniques. Finally, encrypted data may be incriminating in countries when encryption is illegal. This paper presents the encrypted information hiding concept to reduce the risk of using cryptographic algorithms alone. Data hiding techniques embed information into another medium making it imperceptible to others, except for those that are meant to receive the hidden information and are aware of it presence. It focuses on methods of encrypting hidden data in which cryptographic algorithms are combined with the information hiding techniques to increase the security of transmitted data. In such schemes, the secret data is first encrypted, then embedded into cover data to generate 'stego-data', which is then sent through a network or via the Internet. The unauthorized recovery of hidden encrypted data is very difficult because it needs the interceptor to first detect the existence of the hidden information, determine a way of extracting it from the host data and then decrypting it to recover the original information.

The stochastic diffusion process is used as cryptography method. In terms of plaintexts, diffusion ensures that similar plaintexts should result in completely different ciphertexts even when encrypted with the same key [10], [11]. This requires that any element of the input block influences every element of the output block in an irregular way. In terms of a key, diffusion ensures that similar keys result in completely different ciphertexts even when used for encrypting the same block of plaintext. This requires that any element of the input should influence every element of the output in an irregular fashion. This property must also be valid for the decryption process because otherwise an attacker may be able to recover parts of the input from an observed output by a partially correct guess of the key used for encryption. The diffusion process is a function of sensitivity to initial conditions that a cryptographic system should have and further, the inherent topological transitivity that the system should also exhibit causing the plaintext to be mixed through the action of the encryption process.

II. Encrypted Information Hiding

Compared with information hiding in general, the number of publications that have addressed the issue of hiding encrypted information are relatively few. The encrypted information hiding (EIH) algorithms can be categorized into

two types: (i) Spatial domain EIH, where the original host image is directly adjusted, are generally considered simple and often require lower computational cost. However, they can be less robust against attacks such as compression. (ii) Transform domain EIH are achieved by transforming the host image into a suitable transform domain and modifying its coefficients to embed information. Such techniques require higher computational cost and are more complex to implement, although they are considered more robust to various attacks. The following two sections provide an overview of the published literature about EIH techniques based on these methods.

A. Encrypted Information Hiding in the Spatial Domain

In [13] a watermarking scheme is described that combines lossless compression and encryption for medical imaging applications. The authors proposed that a doctor/radiologist is interactively provided with a defined polygonal Region of Interest (ROI). The data is encrypted using Advanced Encryption Standard (AES) algorithm, and then the watermark is compressed using an arithmetic integer compression method. The compressed data is then converted to a binary string and embedded in the image using the bit-plane specified by the user. In [14] the authors proposed a steganographic method using PNG formatted images based on an information sharing technique. The secret image M is divided into shares which are embedded into the alpha-channel of the PNG host image. In [15] the authors introduced the principle of image scrambling and information hiding and proposed a double random scrambling procedure based on image blocks. In [16] a virtually imperceptible image hiding scheme based on vector quantization (VQ) is proposed. The authors goal was to design a high quality and a high capacity image hiding scheme which is based on the VQ compression and a Digital Encryption Standard (DES) based cryptosystem. In [18] an approach to digital watermarking based on the use of cryptography in conjunction with watermarking is presented. The watermark is encrypted by diffusing it with a cipher to produce a scrambled image. The scrambled image is then 'confused' with a host image to hide the encrypted image and produce to the stego-image.

B. Encrypted Information Hiding in the Transform Domain

A steganographic-based approach is proposed in [19] to protect the iris code data by hiding it in a digital image for personal data identification purposes. The iris code data is encrypted using the logistic chaotic map, then the embedding is carried out in DCT domain but changing the mid-to-high frequency band in each DCT block, finally the inverse DCT is applied to generate the stego-image. The extraction process is performed by transforming the stego-image into the DCT domain and selecting the correct coefficients to extract the secret data. The authors in [20] proposed a new hybrid scheme based on a Singular Value Decomposition (SVD), norm quantization and a Modulo-2 approach using two separate procedures to embed two binary watermark images into a grayscale image of size 256×256. The first binary watermark image of size 32×32 is encrypted and then embedded into the host image (after applying SVD matrix norm quantization method to the host). For the second level, the low frequency sub-band from the first level is decomposed using the IWT-Modulu-2 method resulting in four sub-bands of size 64×64. The second binary watermark is then embedded into the second level decomposition. An adaptive digital watermarking algorithm based on chaos and image fusion is presented in [21]. The watermark image is first encrypted using the logistic chaos map, then the adaptive watermark embedding algorithm is applied based on NVF (Noise Visibility Function) and image fusion in the wavelet domain.

III. Encrypted Image Hiding using Stochastic Diffusion

In 'image space', the plaintext is considered to be an image $p(x, y)$ of compact support $x \in [-X, X]; y \in [-Y, Y]$. Stochastic diffusion is that process compounded in the following encryption/decryption algorithms:

Encryption

$$c(x, y) = m(x, y) \otimes_x \otimes_y p(x, y)$$

where

$$m(x, y) = \mathcal{F}_2^{-1}\left[M(k_x, k_y)\right]$$

and $\forall k_x, k_y$

$$M(k_x, k_y) = \begin{cases} \frac{N^*(k_x,k_y)}{|N(k_x,k_y)|^2}, & \mid N(k_x, k_y) \mid \neq 0; \\ N^*(k_x, k_y), & \mid N(k_x, k_y) \mid = 0. \end{cases}$$

The symbols $\otimes_x$ and $\otimes_y$ denote convolution in x and y, respectively, k_x and k_y are the spatial frequencies, $\mathcal{F}_2^{-1}$ denotes the two-dimensional inverse Fourier transform and the function $N(k_x, k_y)$ is taken to be the Fourier transform of a cipher $n(x, y)$.

Decryption

$$p(x, y) = n(x, y) \odot_x \odot_y c(x, y)$$

where $\odot_x$ and $\odot_y$ denote correlation in x and y, respectively. For digital image hiding, we consider a discrete image array $p_{ij}, i = 1, 2, ..., I; j = 1, 2, ..., J$ of size $I \times J$ and discrete versions of the operators involved, i.e. application of a discrete Fourier transform and discrete convolution and correlation sums.

For applications in image watermarking, stochastic diffusion has two principal advantages:

- a stochastic field provides uniform diffusion;
- stochastic fields can be computed using random number generators that depend on a single initial value or

seed which can be used as a private key for the encryption/decryption process.

Detailed information about stochastic diffusion and its mathematical background can be found in [12]

A. Binary Image Watermarking

We consider the plaintext image $p(x, y)$ to be of binary form, such that the output of stochastic diffusion can be binarized to give a binary ciphertext. The rationale for imposing this condition is based on considering a system in which a user is interested in covertly communicating documents such as confidential letters and certificates.

If we consider a plaintext image $p(x, y)$ which is a binary array, then stochastic diffusion using a pre-conditioned cipher $0 \leq m(x, y) \leq 1$ consisting of an array of floating point numbers will generate a floating point output. The Shannon Information Entropy of of any array $A(x_i, y_i)$ with Probability Mass Function (PMF) $p(z_i)$ is given by

$$I = -\sum_{i=1} p(z_i) \log_2 p(z_i)$$

The information entropy of a binary plaintext image (with PMF consisting of two components whose sum is 1) is therefore significantly less than the information entropy of the ciphertext image. In other words, for a binary plaintext and a non-binary cipher, the ciphertext is data redundant. This provides us with the opportunity of binarizing the ciphertext by applying a threshold, i.e. if $c_b(x, y)$ is the binary ciphertext, then

$$c_b(x, y) = \begin{cases} 1, & c(x, y) > T \\ 0, & c(x, y) \leq T \end{cases}$$

where $0 \leq c(x, y) \leq 1 \forall x, y$. A digital binary ciphertext image $c_b(x_i, y_j)$ where

$$c_b(x_i, y_i) = \begin{cases} 1, & \text{or} \\ 0, & \text{for any } x_i, y_j \end{cases}$$

can then be used to watermark an 8-bit host image $h(x, y), h \in [0, 255]$ by replacing the lowest 1-bit layer with $c_b(x_i, x_j)$. To recover this information, the 1-bit layer is extracted from the image and the result correlated with the digital cipher $n(x_i, y_j)$. Note that the original floating point cipher n is required to recover the plaintext image and that the binary watermark can not therefore be attacked on an exhaustive XOR basis using trial binary ciphers. Thus, binarization of a stochastically diffused data field is entirely irreversible.

B. Principal Algorithms

The principal algorithms associated with the application of stochastic diffusion for watermarking with ciphers are as follows:

Algorithm I: Encryption and Watermarking Algorithm

Step 1: Read the binary plaintext image and compute the size $I \times J$ of the image.

Step 2: Compute a cipher of size $I \times J$ using a private key and pre-condition the result.

Step 3: Convolve the binary plaintext image with the pre-conditioned cipher and normalise the output.

Step 4: Binarize the output obtained in Step 3 using a threshold based on computing the mode of the Gaussian distributed ciphertext.

Step 5: Embed the binary output obtained in Step 4 into the host image Least Significant Bit (LSB) to generate the stego-image.

The following points should be noted:

(i) The host image is an 8-bit or higher grey level image which must ideally be the same size as the plaintext image or else resized accordingly using the same proportions.

(ii) Pre-conditioning the cipher and the convolution processes are undertaken using a Discrete Fourier Transform (DFT).

(iii) The output given in Step 3 will include negative floating point numbers upon taking the real component of a complex array. The array must be rectified by adding the largest negative value in the output array to the same array before normalisation.

(iv) For colour host images, the binary ciphertext can be inserted into one or all of the RGB components.

(v) The binary plaintext image should have homogeneous margins to minimise the effects of ringing due to 'edge-effects' when processing the data using Fourier transform.

Algorithm II: Decryption and Extraction Algorithm

Step 1: Read the stego-image and extract its lowest 1-bit layer.

Step 2: Regenerate the (non-preconditioned) cipher using the same key used in Algorithm I.

Step 3: Correlate the cipher with the input obtained in Step 1 and normalise the result.

Step 4: Quantize and format the output from Step 3 to construct the original image.

The following points should be noted:

(i) The correlation operation should be undertaken using a DFT.

(ii) For colour images, the data is decomposed into each RGB component and each 1-bit layer is extracted and correlated with the appropriate cipher.

(iii) The output obtained in Step 3 has a low dynamic range and therefore requires to be quantized into an 8-bit image based on floating point numbers within the range max(array)-min(array).

Figure 1. Certificate with binary watermark (left) and decrypt (right).

IV. Binary Image Watermarking Using Hidden Codes

In order to avoid the LSB extraction, increase the security of the hidden data and improve the robustness of the binary watermarking algorithms discussed earlier, we consider a method of randomizing the cipher bits over multiple host image LSBs as well as randomizing the embedding bits order using different noise distribution (models) as hidden codes. We consider the Gaussian, Log-normal, and Uniform distributions as hidden codes.

A. Gaussian Distribution

Gaussian coding is performed by generating a Gaussian distributed noise pattern, and then randomizing the bit-level of host image embedding according to this distribution. Theoretically, any host image bits can be used for embedding the binary cipher. However, using all 8-bits of the host image reduces image quality, especially over flat or homogeneous regions. Since most of the information is hidden in the first LSB of the host image, extracting the LSB and correlating it with the original cipher (if exposed) may reveal the original data, especially when the number of host image bits used for hiding decreases. We concur that at least 5-bits for hiding the binary cipher should be used thus reducing the amount of information hidden in the LSB. An alternative solution is to use different noise distributions as discussed in the following sections.

B. Log-normal Distribution

In order to reduce the amount of data stored in the first LSB of the host image, a log-normal distribution can be used for bit-level coding. This reduces the potential for unauthorized document access.

C. Uniform Distribution

The uniform distribution provide an alternative to the previous described techniques, with the major advantage being that the binary cipher is scattered uniformly over the host image bits. This makes the host image more secure against LSB extraction attack.

V. Encrypted Grey Scale Image Hiding

The binary image watermarking method discussed earlier is suitable for document authentication, but the lossy nature of the reconstruction generated through binarization of the cipher (illustrated in Figure 1) is not suitable for 8-bit images. In this section we introduce an algorithm for hiding grey scale image in full colour images. Figure 2 shows a block diagram illustrating the proposed approach for hiding an encrypted 8-bit grey scale image into a 24-bit colour host image. Referring to Figure 2, the stochastic diffusion approach is used to encrypt the 8-bit image and embed it into a 24-bit colour host image with a near perfect decryption. In this scheme, the cipher is converted into binary form, then 1^{st} and 2^{nd} Least Significant Bits (LSBs) are ignored and the 3^{rd} and 4^{th} bits are embedded into the two LSBs of the host image's red channel. Similarly, the 5^{th} and 6^{th} bits are embedded into the two LSBs of the host image's green channel, and finally the 7^{th} and 8^{th} bits are embedded into the two LSBs of the host image's blue channel. The inverse process is based on extracting the relevant bits from the associated channels. The extracted bits are then used to re-generate the original cipher and the reconstruction obtained by correlation with the original noise field. A two-steps Hidden Codes approach is applied(*uniform random distribution is used to generate the two codes*). In the first step, code1 is used to shuffle the embedding bits order, so the first secret dataset is not embedded in the first pixel of the host image, but rather in any other pixel based on random locations. In the second step, code2 is applied to scatter the two secret bits over multiple LSBs instead of only two (i.e. 1^{st} to 6^{th} LSBs instead of 1^{st} and 2^{nd}). The hidden codes lead to the following advantages:

(i) The randomized embedding bits order will make it very difficult for intruders to extract the secret bits in correct order without knowing the correct code key.

(ii) The randomized LSBs will make the hidden data more robust and secure to LSB attacks, as losing the 1^{st} and 2^{nd} will only decrease the quality of the reconstructed cipher whilst keeping the ability to recognize the hidden information. Figure 4 shows the result of embedding 8-bit image into a 24-bit host image which is based on the block diagram given in Figure 2.

VI. Encrypted Full Colour Image Hiding

The method of grey scale image hiding can be generalized to embed a 24-bit colour image. The above method is modified to use three full colour images as a host images as shown in Figure 3. The same algorithm is then applied by treating each colour channel of the secret image as a grey scale image and embed it into one of the host images, and hidden codes are applied as discussed earlier with the ability to add another hidden code for shuffling the order of colour channels in the secret image (i.e instead of RGB,

it could be GBR, BRG, etc). In this case the red channel is not necessarily embedded in the first host image, and so on. In order to increase algorithm security, a different key can be used to encrypt each channel. Therefore, the attacker needs to have three correct keys to break the cipher. The inverse process is identical to that discussed in the previous section. The three reconstructed channels are then combined to generate the original 24-bit image. Figure 5 shows an example of the method based on the block diagram given in Figure 3 that embed 24-bit image into three colour host images.

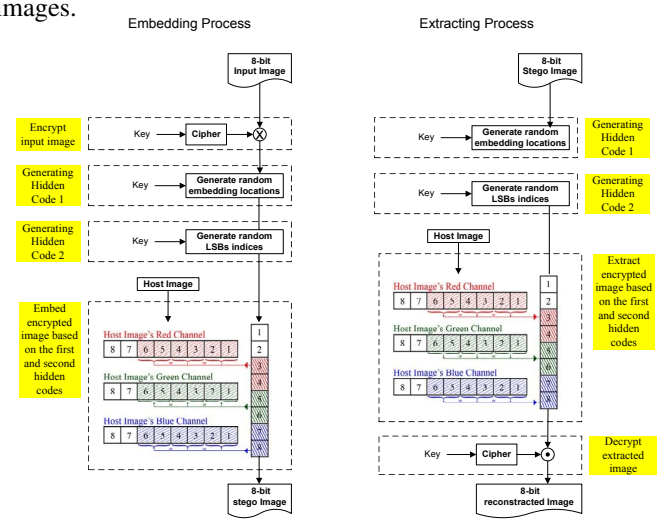

Figure 2. Block Diagram for hiding an encrypted 8-bit image into 24-bit colour host image.

VII. Conclusion

In this paper, the concept of encrypted information hiding has been presented. The use of cryptographic algorithms together with steganography and watermarking methods make it almost impossible for interceptor to recover the encrypted hidden data as this requires the interceptor to detect the existence of the information before attempting to decrypt it. To recover the original data, the attacker needs to first find a way to extract the hidden encrypted information from the stego-data, which requires knowledge of the data hiding codes and the appropriate algorithm/key(s). The exposure of the encryption key(s), the encryption algorithm and the embedding technique along with the hidden codes to those other than the intended receiver is practically impossible. We have considered the application of stochastic diffusion for encrypting image data prior to embedding it into a host image. Embedding a binary watermark into a host image obtained by binarizing a floating point ciphertext, as discussed in Section III, provides a cryptographically secure solution. This is because binarization is an entirely one-way process. Thus, although the watermark may be removed from the stego-image, it can not be decrypted without the recipient having access to the correct encryption key. However, This paper focuses on two key issues: (i)

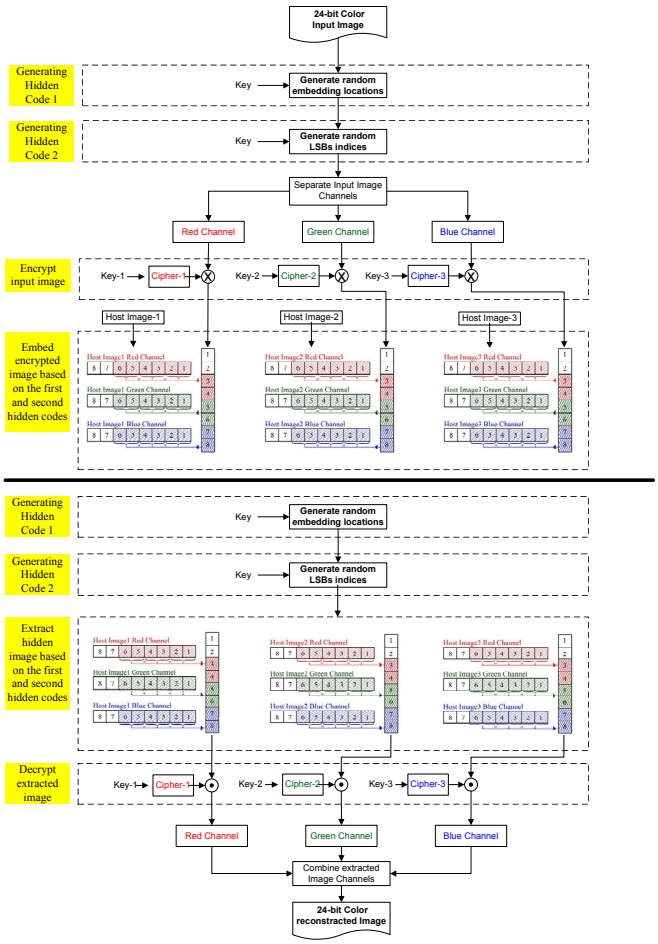

Figure 3. Block Diagram for hiding an encrypted 24-bit colour image into three 24-bit colour host images.

Figure 4. The original image (left), the reconstructed image (middle) and the stego-image (right).

extending the application of stochastic diffusion to hide 8-bit and 24-bit images into a full colour and a set of three full colour images respectively to provide a high fidelity decrypt. Coupled with appropriate key-exchange protocols to initiate cryptographically strong ciphers, the approach provides a generic method of encrypting and hiding high fidelity digital image information. (ii) the use of the Hidden Codes in the embedding process in two phases; the first phase is to shuffle the embedding bits order making, while the second one randomizes the encrypted cipher bits over multiple LSBs making it more secure and robust to certain attacks. However, modifying or destroying the host image

Figure 5. From left to right: the original image, the reconstructed image and the stego-images

LSB (due to compression methods, for example) will not cause full loss of the cipher bits because they are scattered along multiple bits which enables the intended receiver to recover the hidden data.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, New Jersey: Prentice-Hall, 1999.

[2] B. Schneier, *Applied Cryptography (Second Edition)*, Wiley, NewYork, 1996.

[3] Y. H. Chu and S. Chang, *Dynamical Cryptography based on Synchronized Chaotic Systems*, Electronics Letters, 974-975, 1999.

[4] H. J. Highland, *Data Encryption: A Non-mathematical Approach*, Computer Security, 369-386, 1997.

[5] G. Unnikrishnan, J. Joseph and K. Singh, *Optical Encryption by Double-Random Phase Encoding in the Fractional Fourier Domain*, Optics Letters, Vol. 25, Issue 12, 887-889, 2000.

[6] B. H. Zhu, S. T. Liu and Q. W. Ran, *Optical Image Encryption based on Multi-fractional Fourier Transforms*, Optics Letters, 1159-1161, 2000.

[7] R. Tao, Y. Xin and Y. Wang, *Double Image Encryption based on Random Phase Encoding in the Fractional Fourier Domain*, Optics Letters, 16067-79, 2000.

[8] G. Situ and J. Zhang, *Double Random-Phase Encoding in the Fresnel Domain*, Optics Letters, Vol. 29, Issue 14, 1584-1586, 2004

[9] L. Yu, X. Peng and L.Cai, *Parameterized Multi-dimensional Data Encryption by Digital Optics*, Optics Communications, 67-77, 2002.

[10] Ptitsyn, N. V., Blackledge, J. M. and Chernenky V. M., *Deterministic Chaos in Digital Cryptography*, Proceedings of the First IMA Conference on Fractal Geometry: Mathematical Methods, Algorithms and Applications (Eds. J M Blackledge, A K Evans and M Turner), Horwood Publishing Series in Mathematics and Applications, pp. 189-222, 2002

[11] Ptitsyn, N. V., *Deterministic Chaos if Digital Cryptography*, PhD Thesis, De Montfort University, 2003.

[12] Jonathan Blackledge and AbdulRahman Al-Rawi, *Steganography using Stochastic Diffusion for the Covert Communication of Digital Images*, International Journal of Applied Mathematics, vol: 41, issue: 4, pages: 270 - 298, 2011.

[13] M. K. Kundu and S. Das, *Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding*, International Conference on Pattern Recognition, 1457-1460, 2010.

[14] C. W. Lee and W. H. Tsai, *A New Steganographic Method Based on Information Sharing via PNG Images*, 2nd International Conference on Computer and Automation Engineering (ICCAE), 807-811, 2010.

[15] C. Uuefen, L. Junhuan, Z. Shiqing and C. Caiming, *Double Random Scrambling Algorithm based on Subblocks for Image Hiding*, International Conference on Computer and Communication Technologies in Agriculture Engineering, 255-257, 2010.

[16] S. C. Shie, S. D. Lin and J. H. Jiang, *Visually Imperceptible Image Hiding Scheme based on Vector Quantization*, Information Processing and Management, Vol. 46, Issue 5, 495-501, 2010.

[17] Y. Linde, A. Buzo and R. M. Gray, *An Algorithm for Vector Quantizer Design*, IEEE Transactions on Communications, Vol. 28, Issue 1, 84-95, 1980.

[18] J. M. Blackledge, *Authentication of Biometric Features using Texture Coding for ID Cards*, IEEE Computer Society, The Fifth International Conference on Internet Monitoring and Protection , Barcelona, Spain, Vol. 978-0-7695-4023-8, 74 - 83, 2010.

[19] W. Na, Z. Chiya, L. Xia and W. Yunjin, *Enhancing Iris-Feature Security with Steganography*, The fifth IEEE Conference onIndustrial Electronics and Applications (ICIEA), 2233-2237, 2010.

[20] J. Panada, J. Bisht, R. Kapoor and A. Bhattacharyya, *Digital Image Watermarking in Integer Wavelet Domain using Hybrid Techniques*, International Conference on Advances in Computer Engineering (ACE), 163-167, 2010.

[21] Z. Fanm, S. Dongfang and W. Yujing, *Adapting Digital Watermark Algorithm based on Choas and Image Fusion*, Global Congress on Intelligent Systems, Vol. 8, 126-130, 2009.