International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

January- 2015 Volume 2, Issue-1

Email: editor@ijermt.org www.ijermt.org

An Invisible Watermarked Scrambled Image using Arnold Transform

Vikash Yadav
Department of Computer Science & Engg.
Harcourt Butler Technological Institute
Kanpur, India

Punit Kumar Chaubey, Rati Shukla
Department of Computer Science & Engg.
Motilal Nehru National Institute of Technology
Allahabad, India

ABSTRACT-
The increasing globalization (in which an organization enters a new place for trading purpose) led to the transmission of vast amount of digital documents like texts, images, videos or audios over the internet from one point to another. However, some of these documents might be highly confidential and its transmission over the internet must be protected from unauthorized access. In this paper, we have proposed a novel hybrid Arnold transform scheme based on DWT with invisible embedded watermark. In this scheme, we have provided double layer of security by utilizing the multi-resolution property of wavelet using Arnold transform and least significant substitution of invisible watermark. Our scheme provides high security as even after the extraction of first layer, without knowing the extraction algorithm, original image cannot be recovered in its entirety. The proposed scheme is tested on various test images and the obtained results show the effectiveness of the proposed scheme.

Keywords- Arnold transforms, Invisible watermark embedding, discrete wavelet transform**.**

1. INTRODUCTION

Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a "key" the receiver can decode the encrypted message (decrypting) to retrieve the original message. Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes [1] [2]. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric [3]. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text [4]. The keys may be identical or there may be a simple transformation to go between the two keys [5]. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent [6]. Enormous number of transfer of data and information takes place through internet, which is considered to be most efficient though it's definitely a public access medium [7]. The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc. Image encryption, also called image scrambling, produces an unintelligible or disorder image from the original image. The existing image encryption algorithms can be classified into two kinds [8]. One is spatial-based method; the other is frequency-based method. The spatial-based algorithms are usually achieved by swapping the pixel positions or altering pixel values. Arnold transform is an efficient technique for position swapping, and widely applied to image encryption [9]. Arnold transform and exclusive OR operation are used to produce scrambled images. Logistic map exploited to improve the security of Arnold transform. Conventional Arnold transform based schemes have a common weakness that image height must equal image width. Considering pixel value modification, an image encryption scheme based on bit shuffling of individual pixels [10]. It doesn't need iterative computations, and then reduce the run time. A well-known image

encryption algorithm based on frequency domain is designed. However, the decrypted image isn't totally equal to the original image.

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent un-authorized copying directly. Military communications systems make increasing use of track security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving can trace their history back to antiquity; and many of them are surprisingly easy to circumvent.

With this motivation, this paper has the following structure: section II is about DWT and LSB, section III gives information on the proposed algorithm employed for the encryption process, section IV represents the results and discussion and section V concluded the paper.

II. DWT & LSB

Discrete Wavelet Transform (DWT): In several applications, it might be essential to analyze a given signal. The structure and features of the given signal may be better understood by transforming the data into another domain. There are several transforms available like the Fourier transform, Hilbert transform, wavelet transform, etc. The Fourier transform is probably the most popular transform. However the Fourier transform gives only the frequency- amplitude representation of the raw signal. The time information is lost. So we cannot use the Fourier transform in applications which require both time as well as frequency information at the same time. The Short Time Fourier Transform (STFT) was developed to overcome this drawback. However the STFT gives a fixed resolution at all times and this shortcoming was overcome by the development of the wavelet transform. The frequency component of a signal at a particular time instant cannot be exactly determined. This follows directly from the Heisenberg's Uncertainty Principle which states that the momentum and position of a moving particle cannot be exactly determined. Thus the best we can do is to investigate which frequency components exist in any given interval of time. The high frequency components are better resolved in time and low frequency components are better resolved in frequency. This is the reason why the wavelet transform has overtaken the STFT.

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below

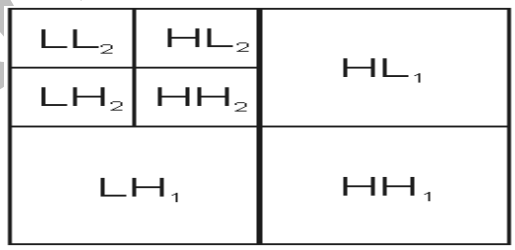


Figure 1: Two Scale 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH,HL,HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

Least Significant Bit (LSB) Modification: The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success.
LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one - fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

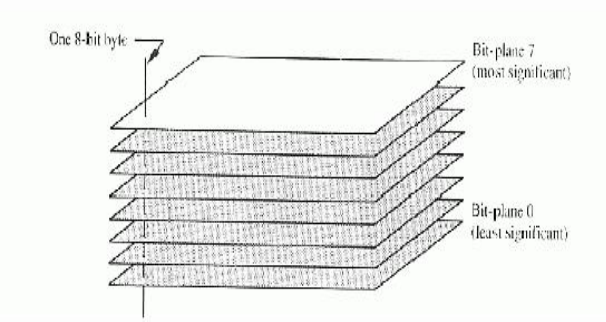


Figure 2: Bit-plane representation of an 8-bit digital image.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key. Security of the watermark would be improved as the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSBs with a constant. Even in locations that were not used for watermarking bits, the impact of the substitution on the cover image would be negligible. LSB modification proves to be a simple and fairly powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

III. PROPOSED ARCHITECTURE OF IMAGE ENCRYPTION

The following flow chart as shown in fig.2 is showing the overview for an image encryption where Arnold map and chaotic method are jointly used. Wavelet transform is also used as edge preserving so that the original information of edges may not loose.
The image encryption architecture is proposed as shown in figure 3, where following steps are processed as:

Step 1: Perform discrete wavelet transform (DWT) to obtain approximation and detail parts.
Step 2: Approximation part of Image is divided into n*n blocks.
Step 3: Each block is shuffled row wise as well as column wise on Approximation part.
Step 4: Apply least significant bit for invisible watermark on Arnold equation for each block of Approximation part. The Arnold transformation that change the coordinate (x, y) to the (x', y') by using formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} mod\ n$$

Step 5: Also, apply invisible watermarked Arnold transform on detail parts.
Step 6: Apply Inverse wavelet transform, to reconstruct the image using encrypted approximation and detail coefficients.

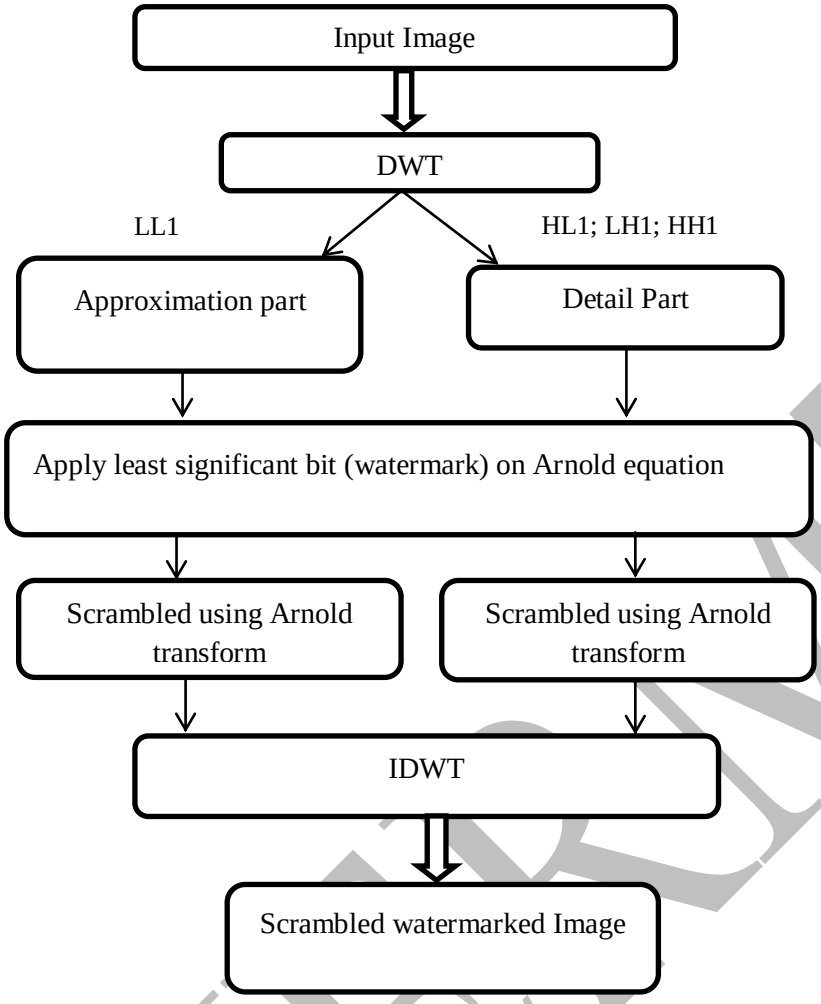
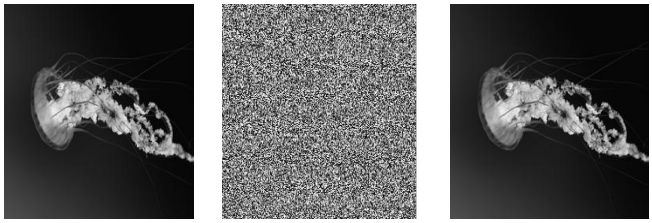


Figure 3: Proposed Architecture of image encryption

In the above proposed algorithm, the two level securities are used. On first level the structure is preserved and encrypted using invisible watermarked using Arnold transform and in second level, each block of approximation part is also encrypted with same method.

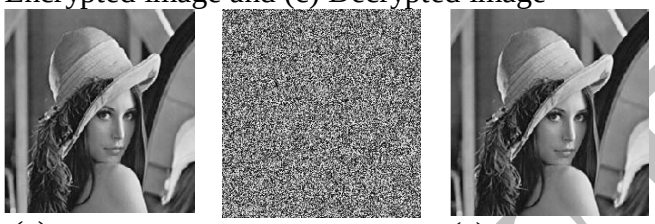
IV. RESULT OF EXPERIMENT AND ANALYSIS

The experimental evaluation is performed on images with size 256x256 using proposed method. Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. Results are shown in fig 4, fig 5, fig 6 and fig 7. Original images are fig 4(a), fig 5(a), fig 6(a) and fig 7(a). Encrypted images are fig 4(b), fig 5(b), fig 6(b) and fig 7(b) and Decrypted images are 4(c), fig 5(c), fig 6(c) and fig 7(c).



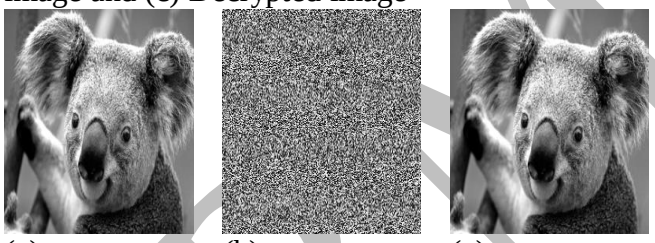
(a) (b) (c)

Figure 4: (a) Original image: Jellyfish (b) Encrypted image and (c) Decrypted image



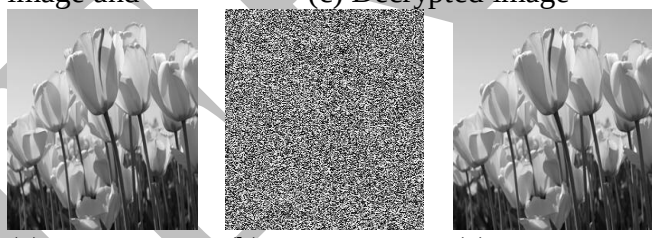
(a) (b) (c)

Figure 5: (a) Original image: Lena (b) Encrypted image and (c) Decrypted image



(a) (b) (c)

Figure 6: (a) Original image: Koala (b) Encrypted image and (c) Decrypted image



(a) (b) (c)

Figure 7: (a) Original image: Tulips (b) Encrypted image and (c) Decrypted image

Mean error for original and decrypted images are calculated and given in Table 1. From table 1, we can analyze that the value of mean error is very less, near to zero. It means our decrypted image is almost same as original image.

Table 1: Mean error

Input Images	Mean error
Jellyfish	0.0923
Lena	0.0162
Koala	0.0634
Tulips	0.0183

V. CONCLUSION

The proposed encryption algorithm uses an invisible watermark based on Arnold transform for scrambling the image. Invisible watermarking is more secured using Arnold transform. And structure is also secured as watermarked as well as scrambled. Block wise shuffling and secured watermark is improving the accuracy of our proposed algorithm. Results are also indicate, that proposed algorithm is fast and prevents from the attacks. An initial key is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly. This guarantees the security of the proposed technique against brute-force attacks to some extent.

REFERENCES

1. C.Y. Lin, M. Wu, J.A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images", IEEE Transactions, Image Processing, Vol. 10, pp. 767-782, May 2001.
2. C. Li and G. Chen, "On the security of a class of image encryption schemes," Proceedings of the IEEE International Symposium on Circuits and Systems, 2008.
3. S. Li, C. Li, G. Chen, and X. Mou, "Cryptanalysis of the RCES/RSES image encryption scheme," available online at http://eprint.iacr.org/2004/376 on 15 Oct. 2008.
4. Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm" Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.
5. M. A. BaniYounes and AmanJantan, "Image Encryption Using Block-Based Transformation Algorithm"IAENG, 35:1, IJCS_35_1_03, February 2008.
6. IsmetOzturk and AbrahimSogukpinar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology 3 2005.
7. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.
8. W.Stallings,Cryptography and network security:Principles and Practice.Prentice hall,2010,vol.998.
9. I.J. Cox and M.L. Miller,"A review of watermarking and the importance of perceptual modeling", Proceedings of Electronic Imaging'97, February 1997.
10. J. Fridrich, 2 Lt Arnold C. Baldoza, and Richard J. Simard "Robust digital watermarking based on key-dependent basis functions" 2nd Information Hiding Workshop, Portland OR, April 15–17, 1998.