ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Auto Key Elliptical Cryptography Method For The Encryption And Decryption of An Image

[I]Poonam, [II]Er. Kapil Arora
[I]M.Tech Student, [II]Assistant Professor
[I,II]Dept. of ECE, RPIIT, Karnal, Haryana, India

Abstract
Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. The proposed work is supported on the GUI model which gives a practical implementation of the work. The work is implemented on the MATLAB software and different aspects have been considered. The proposed method is cost effective, highly authentic, flexible and reliable.

Keywords
Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain, Least Significant Bit, GUI.

I. Introduction

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly with the introduction of Marc Andreessen's Mosaic web browser in November 1993, and it quickly became clear that people wanted to download pictures, music, and videos. The Internet is an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high-capacity digital recording devices. When the only way the average customer could record a song or a movie was on analog tape, pirated copies were usually of a lower quality than the originals, and the quality of second-generation pirated Copies (i.e., copies of a copy) was generally very poor. However, with digital recording devices songs and movies can be Recorded with little, if any, degradation in quality.

A. Digital Watermarking

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark.

The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust" we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. In some cases the watermark may need to be fragile.

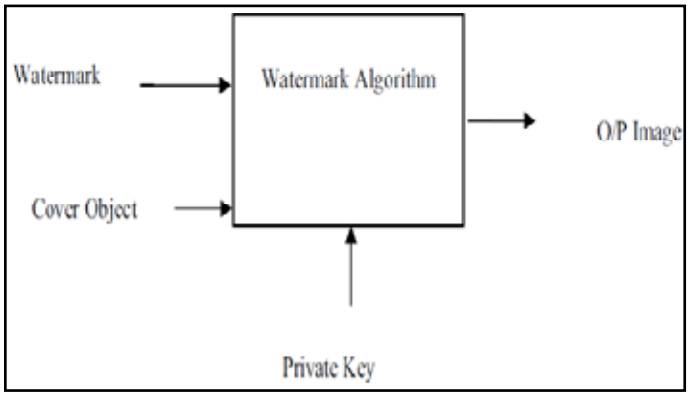


Fig. 1.1: General watermarking Diagram

II. Literature Survey

DCT coefficients of the original image, and the inverse DCT was taken to retrieve the watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, and rescanning. Xia, Boncelet, and Arce proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT).Bas, Chassery, and Davoine introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT. The watermark was added to the collage map to produce a marked image. Results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

III. Problem Formulation

Watermark robustness is one of the major characteristics that influence the performance and applications of digital image

watermarks. Robustness in this context means the ability of a watermark to resist common image processing. Watermarks can be categorized into three major groups based on their robustness: robust, fragile, and semi-fragile watermarks. Robust watermarks should be detected successfully in images that have been through manipulative distortions. Adversely, fragile watermarks are very sensitive and easily destroyed by image modifications. In the middle of both extreme ends are the semi-fragile watermarks. They can resist legitimate changes while being sensitive to severe tampering. Copyright protection concerns the positive identification of content ownership in order to protect the rights of the owner.

1. Algorithm for watermarking

Step 1- Check the length of the watermark image to know how many copies will be embedded in the first LSB and if it will embed in the second LSB.
Step 2- Embedding the length of the watermark image in the first LSB.
Step 3- Convert the watermark image to bits.
Step 4- Inverse the watermark bit.
Step 5- Check the coordinate of X, if it is odd, the algorithm will add 1 to X, and if it is even, the algorithm will subtract 1 from X.
Step 6- Embed the watermark bit in the first LSB.
Step 7- Go to 4 until finishing the entire watermark.

IV. Proposed Approach

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.

1. Spread Spectrum Technique

Recent development in this technique has utilized the concept of Spread-Spectrum technique prevalent in Communications. Arguably, one of the most robust technique, here we consider a new non-linear technique of watermarking.

2. Algorithm for Watermarking using SST technique

Input:
Cover image
Watermark text
output
Watermarked image
Step1: Read watermark text converts it in matrix
Step2: Find mean and variance
Step3: Normalized the texts
y(i)=(y(i)-mean_mesg)/var_mesg;
Step4: Read Cover Image
Step5: Find DCT of cover image then mean and variance.
Step6: normalized the cover image.
Step7: Count Neighbour and set alpha more the neighbour more the alpha
alpha(i,j)=mean(neigh)*y(length);
Step8: Insert watermark on cover image
J(i,j)=J(i,j)*alpha(length);
Step9: Denormalized the watermarked image.
Step 10: Result image is watermarked image

3. Algorithm for Dewatermarking using SST technique

Input:
Watermarked Image.
Output:
Watermark Image

Step1: Denormalized watermarked image
Step2: Inverse DCT
Step3: Calculate variance
imgd_var = var(Jd);
Calculate Mean
imgd_mean = mean(Jd);
Step4: dw(i,j)=Jd(i,j)*imgd_var(i) + imgd_mean(i);
Step5: w(i)=(y(i)*var_mesg)+ mean_mesg;
Step6: Convert matrix into text

V. Results And Analysis

1. Encryption design layout

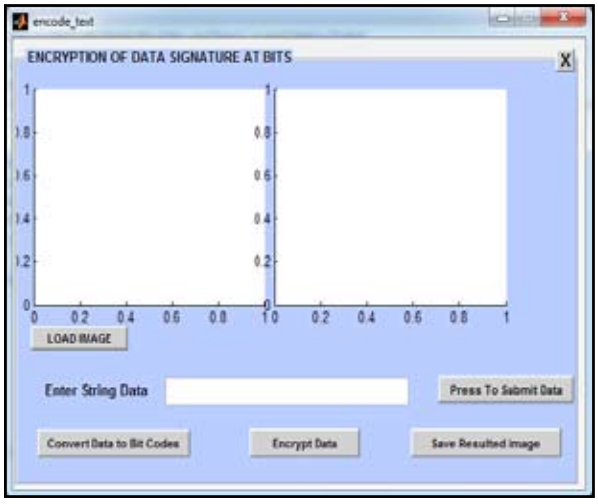


Fig. 5.1: GUI layout

2. Loaded image

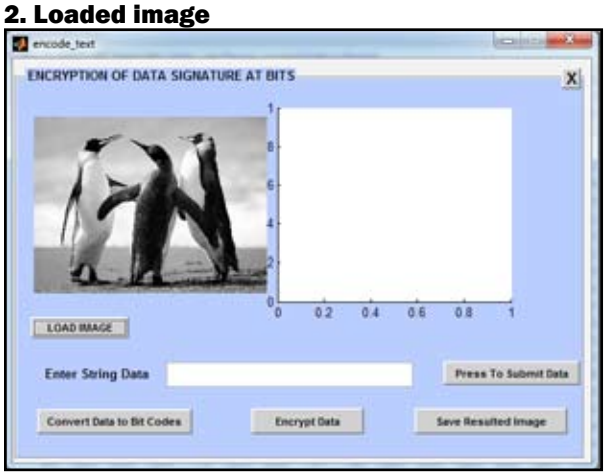
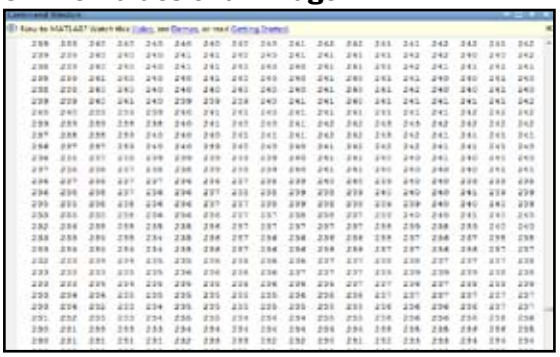


Fig. 5.2: loaded original image

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

3. Pixel values of an image



4. Encrypted image

Fig. 5.3: GUI with encrypted image

A. String to Binary conversion

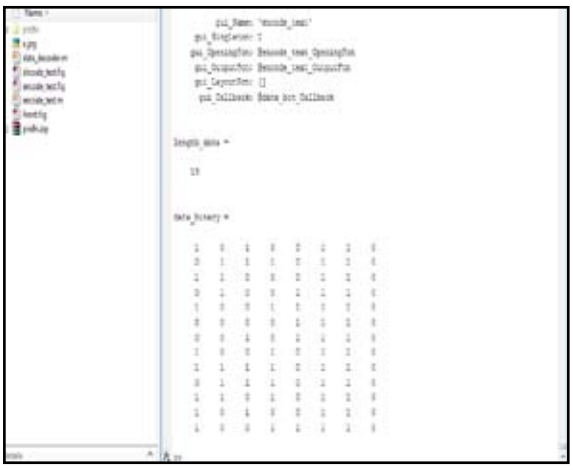


Fig. 5.4 : Snapshot of command window

5. Recovered image

Fig. 5.5: Recovered Image

On clicking the save resulted image button the axes show the original image that was sent from the transmitter. In the proposed work we have used automatic privacy keys at the receiver side to dewater marked the image. This would reduce the complexity, cost, simulation time of the project. Different images can be sent from the sending part and the same way the same image can be obtained without any loss.

A. Function Layout

Fig. 5.6: Watermarked functions

VI. Conclusion And Future Scope

Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. These can be described by many different methods. Two broad categories for these methods were described in this thesis. The watermark is inserted in the most perceptually significant sub-image, thus eliminating chances of its being subjected to severe digital attacks, which will reduce the value of the image. The experimental results presented on the quality and recognizability demonstrates the performance of our method under various attacks. Of course the examples provided in this thesis are only a small sample of the many different approaches to watermarking. Examples of other approaches that have not been mentioned include those which operate in the frequency domain and take advantage of DCT.

The future work can be further extended with different formats of image using different encryption keys. By first encoding the

message with a pseudorandom sequence, we could increase the security of the message. If the encoder uses the pseudorandom sequence with the message as a seed to select which segments are encoded, the decoder can only find what the original message was if he also has the sequence length.

References

[1] *Menezes, A.J., et al., Handbook of Applied Cryptography. 1996: CRC Press. 780 pages.*
[2] *Cox, I.J., M.L. Miller, and J.A. Bloom, Digital Watermarking. 2002: Morgan Kaufmann.*
[3] *Geradts, Z.J., et al. Methods for identification of images acquired with Digital cameras. In Enabling Technologies for Law Enforcement and Security. 2001: SPIE.pp.505-512*
[4] *Liu, K.J.R., et al., Multimedia Fingerprinting Forensics for Traitor Tracing. EURASIP Book Series on SP&C. 2005: Hindawi Publishing Corporation.*
[5] *Kundur, D. and D. Hatzinakos. Semi-blind image restoration based on telltale watermarking. in Conference Record of the Thirty-Second Asilomar Conference on Signals, Systems & Computers 1998. 1998. Pacific Grove, CA, USA: IEEE. pp.933-937 vol.2*
[6] *Lin, C.-Y., SARI 1.0: Performance Charts and Technical Description, 2000,online at http://www.ctr.columbia.edu/~cylin/auth/performchart.html, last accessed 11 September 2006*
[7] *Lin, C.-Y. and S.-F. Chang. SARI: Self-Authentication-and-Recovery Image Watermarking System. in ACM Multimedia 2001. 2001. Ottawa, Canada: ACM Press.pp.628-629*
[8] *Lyu, S., Natural Image Statistics for Digital Image Forensics, in Department of Computer Science. Ph.D. thesis, Dartmouth College: New York.2005*
[9] *R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," Proc. IEEE Int. Conf. on Image Processing, Nov. 1994, vol. II, pp. 86-90.*
[10]. *I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997*
[11]. *X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.*
[12]. *F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.*
[13]. *D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 544-547.*
[14] *J. Delaigle, C. De Vleeschouwer, and B. Macq, "Psychovisual Approach to Digital Picture Watermarking," Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640, July 1998.*
[15] *S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573-586, May 1998.*
[16] *P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.*
[17] *C.-S Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication", PhD Thesis, Queensland University of Technology, Australia, March 2007.*
[18] *A. Khan, "Intelligent Perceptual Shaping of a Digital Watermark", PhD Thesis, Faculty of Computer Science, GIK Institute, Pakistan, 2006.*
[19] *A. B. Watson, G. Y. Yang, J. A. Solomon, J. Villasenor, "Visibility of Wavelet Quantization Noise", IEEE Transactions on Image Processing,Vol. 6, No. 8, pp. 1164-1175, August 1997.*
[20] *G.J. Yu, "Digital Image Watermarking for Copyright Protection and Authentication", PhD Thesis, National Central University, Taiwan, R.O.C, 2001.*