International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

Advanced Stegnography for Fingerprint Analysis and Authentication

G.Prasanna Lakshmi,Research Scholar,Gitam University
Dr. J.A.Chandulal,,Professor of CSE,Gitam University
Dr. Gopala Krishna Patro,Principal, BVMIT

Abstract

With the wide spread utilization of fingerprint based smart card identification system, establishing the authenticity of data itself has emerged as an important issue. This paper proposes a method based on the Steganography. Two techniques, namely encryption and PRNG based embedding are used in LSB embedding to enhance security. Also the performance of the scattered LSB embedding technique is compared with that of sequential embedding and is found to be superior in terms of PSNR and MSE values.

Index Terms: fingerprint, smart card identification, authenticity, stegnography, encryption, embedding and histogram.

Introduction

Steganography is the art of hiding a message signal in a host signal, such as audio, video, still images and text document without any imperceptible distortion of the host signal. The basic idea of image data hiding is to hide the secret image under the camouflage of the cover-image. There are, in general, two approaches that can be used for image data hiding. One approach is the spatial domain techniques and the second approach is the transform domain techniques. Spatial domain techniques usually embed the bits of the message directly into the least significant bits (LSBs) of the pixels of the cover image. This encoding is the simplest steganographic techniques, but the stego-image is sensitive, and not robust to operations such as blurring, cropping, lossy compression, and addition of noise. The second type of stegnography method, is the frequency domain method, which is based on embedding the coefficients in the frequency domain (i.e., Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT)). This type of technique is more robust with regard to common image processing operations and lossy compression. Another type of method is that of adaptive Steganography which adapts the message embedding technique to the actual content and features of the image. For added security, the biometric application stores and verifies users' fingerprint information directly on the Stegnography. The fingerprint information never leaves the card and is never stored in a database, thus protecting users' digital identities. Privacy issues and security risks associated with other biometric authentication methods are mitigated because the fingerprint credentials are stored and validated on the Stegnography which is constantly in the user's possession.

Stegnography systems embedded with biometric data As shown in Figure, Stegnography systems embedded with biometric data such as fingerprint have enable more reliable applications such as home entertainment, personal identification and prepayment service. Stegnography can be used as a unique portable identity token for a wide area of personalized security services within business and government organizations. They support contact and contact-less communication interfaces and multiple authentication, identification, and authorization methods, including single key, one time passwords (OTP), digital certificates (PKI), and biometrics. In addition to strengthening the security, Stegnography also provides convenience to users and administrators with significant cost savings through consolidation of security services using a single identity credential.

II) Existing methods

The classic LSB steganography method which embeds message i.e. fingerprint into cover image, uses message bit stream to replace the cover image's least-significant bit (LSB) sequentially. A major goal in image steganography is to preserve the statistical properties of the host image to thwart statistical based steganalysis, however, these classical LSB steganography methods [1] introduce some distortions into the host signal's and changes the statistical properties, which indicates that certain manipulations of the signal.

III) Proposed Method

In order to overcome the errors of the above classical LSB methods, this paper proposes a technique which performs scattered LSB embedding to preserve the histogram of the host signal. For added security, this biometric application stores and verifies users' fingerprint information directly on the Stegnography. The fingerprint information never leaves the card and is never stored in a database, thus protecting users' digital identities. Privacy issues and security risks associated with other biometric authentication methods are mitigated because the fingerprint credentials are stored and validated on the Stegnography which is constantly in the user's possession. This paper proposes a method in which the cover images, which are 8 bit colour images, are used. The fingerprint images, which are to be hidden, are taken from FVC2004 database. The header which has information about the hidden file, its size and filename and the fingerprint image to be hidden are encrypted with an encryption algorithm, and the given password is used, before being written in the cover image. . The fingerprint image bits are not embedded in a linear fashion; but a pseudorandom number generator (PRNG) is used to choose the location to embed each bit of the fingerprint. The values generated by the pseudo-random number generator depends on the password; such that it is not possible to read the secret data in order to get the hidden file (not even the encrypted version), without knowledge of the password [2]. This encrypted image is stored by using the process of Stegnography and during authentication; the fingerprint can be extracted from the cover image. The cover image can be the photo of the person, so that it gives visual authentication [3].

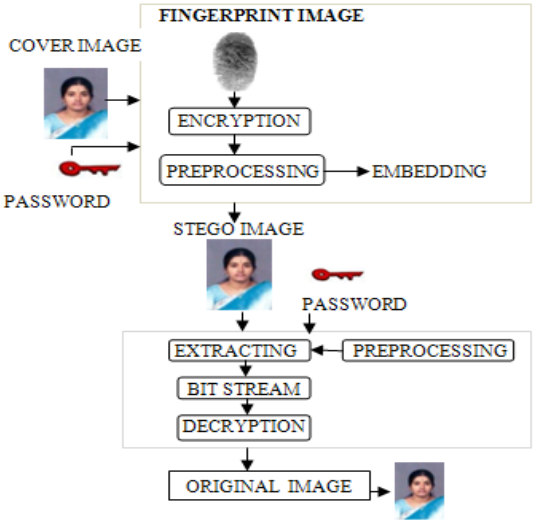
Embedding Process:

1. Read the input cover image.
2. Read fingerprint image to be hidden in the cover image.
3. Obtain password from user.
4. Encrypt the fingerprint image using the proposed method.
5. Generate pseudo random number based on password and calculate the LSB's to hide the image.
6. Hide the fingerprint image in the cover image.
7. Resulting image is called the stegno image.

Retrieving Process:

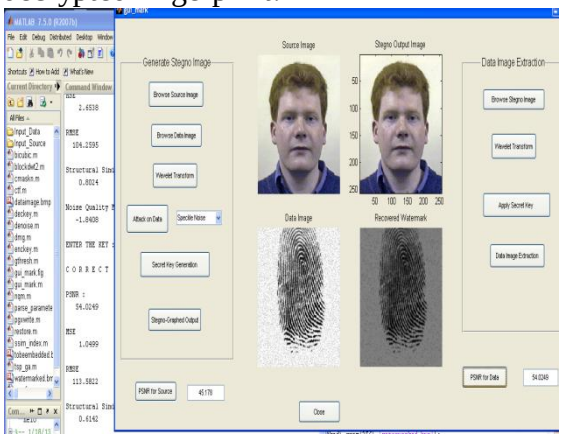
1. Read stegno image
2. Obtain password from user.
3. Generate pseudo random number based on password to calculate the LSB's to know the location, where fingerprint was hidden.

4. Retrieve the fingerprint image.
5. Decrypt the fingerprint image
6. Resulting image is the original cover image.



IV) RESULTS

The results of the proposed method is as shown below for one cover image and the fingerprint image, the above screen shot of the GUI also shows the decrypted fingerprint.



The proposed method is tested for two important and most significant fidelity criteria, PSNR and MSE and the results have been tabulated along with a comparison of the existing method.

Results of 10 database images in terms of PSNR values

Data Base	Existing Extraction(DB)	Proposed Extraction(DB)
1	45.17	54.02
2	44.61	52.85
3	45.21	54.65
4	43.56	55.74
5	42.89	53.54
6	46.23	55.45
7	44.85	53.64
8	42.9	52.25
9	43.65	53.65
10	42.7	52.1

Results of 10 database images in terms of MSE values

Data Base	Existing Extraction(DB)	Proposed Extraction(DB)
1	2.65	1.05
2	2.54	1.21
3	2.32	1.1
4	2.7	1.25
5	2.56	1.07
6	2.21	0.95
7	2.35	1.15
8	2.48	1.23
9	2.67	1.32
10	2.32	1.12

V) Conclusion

In this paper, a new method for advanced stegnography for fingerprint analysis and authentication has been proposed and the output results have been compared with the existing methods in terms of fidelity criteria PSNR and MSE. The results show that the proposed method gives better results in terms of both PSNR and MSE.

VI) References

[1]. N. K. Ratha, J. H. Conne, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images", Proc. of Int'l Conf. on ACM Multimedia 2000 workshops, pp. 127-130, Los Angeles, California, 2000.
[2]. J.K. Yan and D. J. Sakrison, .Encoding of images based on a two component source model.,

IEEE Trans. Commun., Vol. 25, PP.1315-1322, Nov. 1997
[3]. Arithmetic Coding For Data Coiupression Ian H.Willen,Radford M.Neal and John G.Cleary.
[4] X. Li, T. Zeng, and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K., 2008, pp. 133–138.
[5] Y. Q. Shi et al., "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 6–8, 2005, pp
[6] S. Dumitres cu, X.Wu, and Z.Wang, "Detection of LSBsteganography via sample pair analysis," IEEE Trans. Signal Process., vol. 51, no. 7, pp. 1995–2007, Jul. 2003.
[7] A.D. Ker, "A general framework for structural steganalysis of LSB replacement," in Proc. 7th Int. Workshop on Information Hiding, 2005, vol. 3427, pp. 296–311.
[8] D. Ker, "A funsion of maximum likelihood and structural steganalysis," in Proc. 9th Int. Workshop on Information Hiding, 2007, vol. 4567, pp. 204–219.
[9] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," Proc. SPIE Electronic Imaging, vol. 5020, pp. 131–142, 2003.
[10] A.D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.
[11] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels," in Proc. IEEE Int. Conf. Image Processing, Oct. 16–19, 2007, vol. 1, pp. 401–404.
269–272.
[12] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.
[13] A.Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Proc. 3rd Int. Workshop on Information Hiding, 1999, vol. 1768, pp. 61–76.
[14] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. 2001.