Analysis of Image Hiding Process with Biometric Authentication Using LSB Stegnography & Mixed Key Cryptography

Gaurav Sharma, Vipra Bohra

Abstract— **The implementation of a system that amalgamates encryption with biometric authentication to provide high level security is the sole purpose of this paper. The system is based on the hybrid algorithm of the LSB stegnography and mixed key cryptography which is being secured by a key which is of variable length and also finger printing is used in order to generate key and to provide better security. As the proposed work can be applied on both text as well as images.The propose work make use of biometric thinning and binarization in order to generate minutia which is helful in generating key. Based on hybrid algorithm, LSB stegnography and cryptoghaphy is being used.**

Index Terms— **Biometric, Cryptography, Steganography.**

I. Introduction

In the present scenario, where security is the major concern in the recent era, encryption is one of thr methods through which we can save our data or information & can provide a security. In our proposed work, we have used biometric authentication as our key. As we know, no two persons can have the same fingerprint due to its unique quality. So here in the proposed work we are using finger prints as our key.The system flow of the process is the combination of steganography and cryptography of the covert image transmission with the biometric authentication. The minutia is generated as a variable key and the covert image is hidden in cover image using LSB steganography. The steganographed image is encrypted using cryptography with the variable length biometric key. The recovery exist at receiver end with the stego image is created and decrypted following recover age of cover & covert image. Covert channels area unit extremely onerous to put in in real systems, and may usually be detected by observation system performance. Additionally, they suffer from a coffee SNR and low knowledge rates (typically, on the order of a couple of bits per second).They will even be removed manually with a high degree of assurance from secure systems by well established covert channel analysis methods.

Covert channels area unit distinct from, and sometimes confused with, legitimate channel exploitations that attack low-assurance pseudo-secure systems victimisation schemes like steganography or perhaps less subtle schemes to disguise prohibited objects within legitimate info objects[1-3].The legitimate channel misuse by steganography is specifically not a kind of covert channel. Covert channels will tunnel through secure operative systems and need special measures to regulate. Covert channel analysis is that the solely well-tried thanks to management covert channels in contrast, secure operative systems will simply stop misuse of legitimate channels, therefore distinctive each is vital. The LSB steganography being least significant bit, the thought behind LSB embedding is that if we modify the last bit worth of a picture element, there won’t be a lot of visible amendment within the color. In cryptography, a hybrid cryptosystem is one which mixes the convenience of a public-key cryptosystem with the potency of a symmetric-key cryptosystem. Public-key cryptosystems are convenient therein they are doing not need the sender and receiver to share a typical secret so as to speak firmly (among different helpful properties). However, they typically have confidence difficult mathematical computations and ar therefore usually way more inefficient than comparable symmetric-key cryptosystems. In several applications, the high price of encrypting long messages during a public-key cryptosystem is preventive. The biometric authentication if each samples of the biometric information match, authentication is confirmed. Typically, identity verification is employed to manage access to physical and digital resources like buildings, rooms and computing devices.

II. METHODOLOGY

For, the propose work, we have used finger print image to generate a key ,which is a unique random variable generated in order to encrypt and decrypt the cover image as well as covert image. For the stegnography , the LSB stegnography is used in order to get the stegnographed image. Then, use of mixed key cryptography to encrypt the image. For the finger print we have used binarization as well as thinning to generate a unique key. Now, we will use this finger print and get the minutia from the thinning. From the minutia, flash minutia is removed and then we can export the minutia.

Gaurav Sharma, Electronics & Communication,Yagyavalkya Institute of Technology,Jaipur,India.
Vipra Bohra,Electronics & Communication,Yagyavalkya Institute of Technology,Jaipur,India

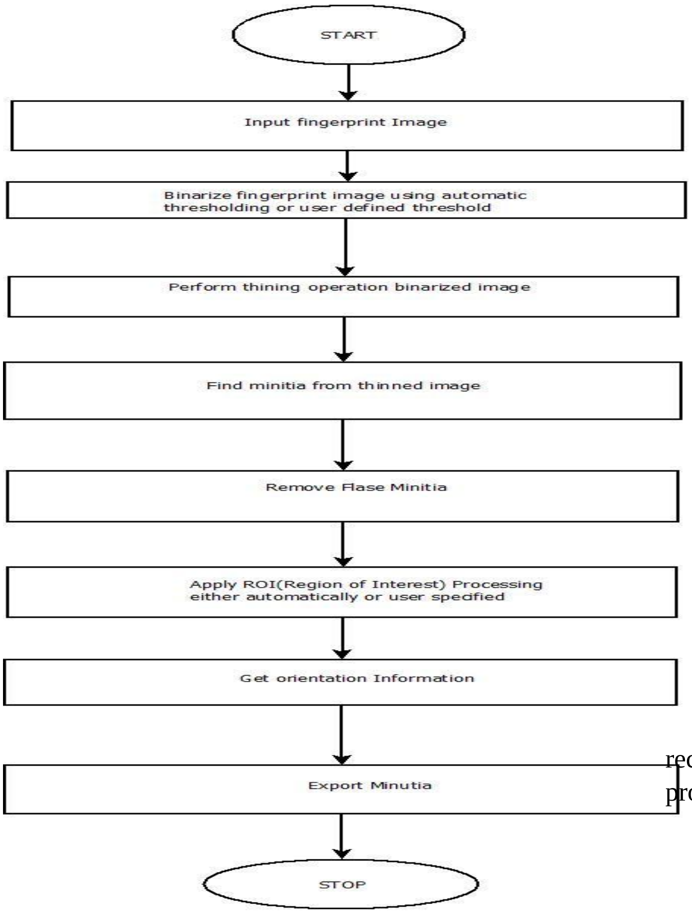

START
Input fingerprint Image
Binarize fingerprint image using automatic thresholding or user defined threshold
Perform thining operation binarized image
Find minitia from thinned image
Remove Flase Minitia
Apply ROI(Region of Interest) Processing either automatically or user specified
Get orientation Information
Export Minutia
STOP

Fig 1:Unique key generation

III. RESULT

We below show the covert image transmission over an unsecured channel using hybrid stegnography & cryptography with biometric authentication.

Step 1: We can observe that a image file is loaded by clicking on file menu option.

Step 2: We can see the original image of finger print which we will binarize & thining will be done manually and automatically.

Step 3: We generate minutia and variable length key with the length and width of fingerprint image.

Step 4:We then apply neighbourhood operation by clicking on find minutia option. On the thining option we see thining image of finger print perfectly.

Step 5:When we click on find minutia option then we can see the minutia image of finger print that we have used. The region of interest button is shown as key.

Step 6:The covert image is being hidden inside cove image and being stegnographed and encrypted.

Step 7:The recovery process exists at receiver end and covert image is recovered.

In this window we can see covert image by click on recover covert image. That is our secure image.

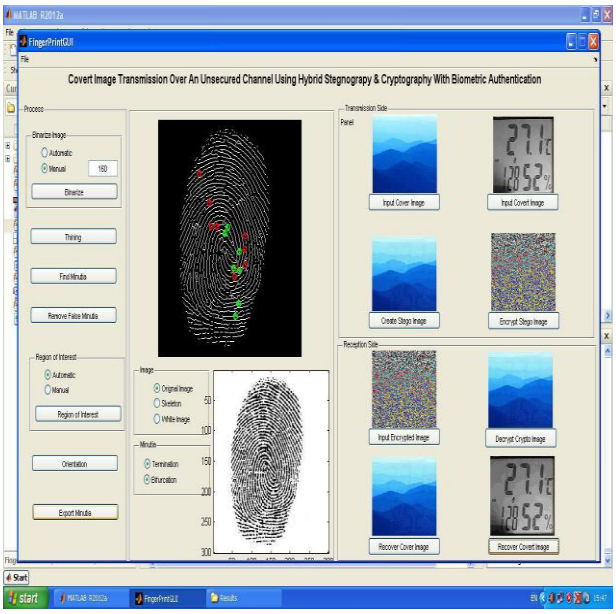
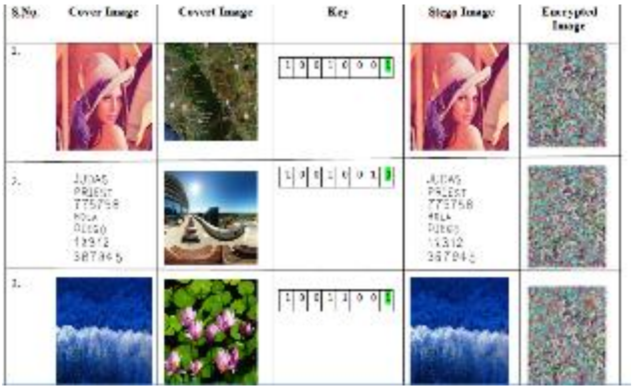


Fig 2:Panel view of covert image recovered

Analysis: The result so obtained may be made to send & receive the exact the same covert image through the procedure as explained.



S.No.	Cover Image	Covert Image	Key	Stego Image	Encrypted Image
1.			1 0 0 1 0 0 0 1		
2.	JUDAS PRIEST 775758 HOLA DIEGO 12912 387845		1 0 0 1 0 0 1 1	JUDAS PRIEST 775758 HOLA DIEGO 13312 367845	
3.			1 0 0 1 1 0 0 1		

Fig 3: Transmitter side

As shown above the panel view of the transmitter side the images of the cover image & covert image are of the different format viz RGB ,text etc and the random key is generated to encrypted the image.

The recovery exists at the receiver end with the same encrypted image & key the cover and finally the covert image is obtained as shown below.

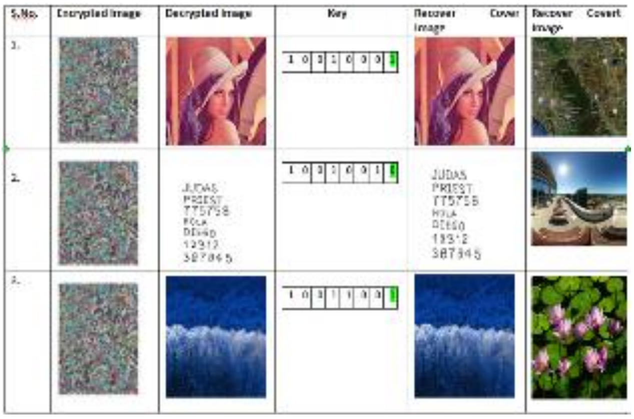

S.No.
Encrypted Image
Decrypted Image
Key
Recover Cover Image
Recover Covert Image
1.
2.
3.
JUDAS
PRIEST
775758
HOLA
DIEGO
13912
387845

Fig 4: Receiver side

IV. CONCLUSION

We have proposed a method using biometric authentication by applying the LSB stegnogrphy and cryptography on the text and images. As in the stegnography it also covers the multi object cover image in spite of the single stage stegnography. As by using LSB stegnography , we will hide our covert image into the cover image and through the mixed key cryptography , we will generate a unique random variable which will act as a key to encrypt the image and further through the decryption process, we will retrieve our cover as well as covert image .Also, security being major concern now days, we have used finger print as a base to provide security which works well for the process. In this way we are achieving high level security for the proposed method.

REFERENCES

[1] O. Habbouli, and D. B. Megherbi “A Secure, Self-recovery, and High Capacity Blind Digital Image Information Hiding and Authentication Scheme Using DCT Moments” IEEE 2017.

[2] Amit A. Ghadyalji, Sagar S. Bandnerkar “Implementation of Reversible Data Hiding Using Suitable Wavelet Transform For Controlled Contrast Enhancement” International Journal on Recent and Innovation Trends in Computing and Communication 2017.

[3] Khan Farhan Rafat, Muhammad Junaid Hussain “Secure Steganography for Digital Images” International Journal of Advanced Computer Science and Applications 2016.

[4] TOSHANLAL MEENPAL “DWT-based blind and robust watermarking using SPIHT algorithm with applications in tele-medicine” Indian Academy of Sciences 2016.

[5] Mehdi Hussain 1,2, Ainuddin Wahid Abdul Wahab 1,*, Noman Javed 3 and Ki-Hyun Jung 4,* “Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images” MDPI 2016.

[6] D. Chakra Rao1 , Dr.RudraPratap Das2 “Hybrid Data Hiding Scheme in Images using DWT DCT and SVD” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2015.

[7] Yanping Zhang1,2, Juan Jiang1,2, Yongliang Zha1,2, Heng Zhang1,2, Shu Zhao1, “Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images” International Journal of Intelligence Science 2013.

[8] Sushila Kamble1, Vikas Maheshkar2 , Suneeta Agarwal3 , Vinay K Srivastava4 “DWT-SVD BASED SECURED IMAGE WATERMARKING FOR COPYRIGHT PROTECTION USING VISUAL CRYPTOGRAPHY” Computer Science & Information Technology (CS & IT) 2012.

[9] Do Van Tuan, Tran Dang Hien, Pham Van At “A Novel Data Hiding Scheme for Binary Images” International Journal of Computer Science and Information Security 2012.

[10] 1 Shabir A. Parah, 2Javaid A. Sheikh, 3G.M. Bhat “High Capacity Data Embedding using joint Intermediate Significant Bit (ISB) and Least Significant Bit (LSB) Technique” Journal of Information Engineering and Applications 2012.

[11] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal “A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier” Journal of Global Research in Computer Science2011.

[12] D. Saravanan, A. Ronald Doni & A. Abisha Ajith “Image Information Hiding: An Survey” The Standard International Journals (The SIJ)2013.

[13] Deepali Singla, Dr. Mamta Juneja “New Information Hiding Technique using Features of Image” JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE 2014.

[14] Joshua R. Smith and Barrett O. Comiskey “Modulation and Information Hiding in Images” Proceedings of the First Information Hiding Workshop 1996.

[15] John D. Strunk, Garth R. Goodson, Adam G. Pennington, Craig A.N. Soules, Gregory R. Ganger “Intrusion Detection, Diagnosis, and Recovery with Self-Securing Storage” USENIX 2002.

[16] Marco Grangetto, Member, IEEE, Enrico Magli, Member, IEEE, Gabriella Olmo, Senior Member, IEEE “Distributed Arithmetic Coding” IEEE COMMUNICATIONS LETTERS 2007.

[17] Mehdi Hussain , Ainuddin Wahid Abdul Wahab , Noman Javed and Ki-Hyun Jung “Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images” Symmetry 2016.

[18] Santi P. Maity, Dr. Uma Bhattacharya , Dr. Malay K. Kundu “Studies on Data Hiding in Digital Media for Secured Communication, Authentication and Content Integrity” BESU2007.

[19] Ahmed Ibrahim , Arwa Zabian “Algorithm for Text Hiding in Digital Image for Information Security” IJCSNS International Journal of Computer Science and Network Security 2009.

[20] TOSHANLAL MEENPAL “DWT-based blind and robust watermarking using SPIHT algorithm with applications in tele-medicine” Sådhana 2016.