International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 5, Issue 1, May. 2016, pp.806-810, ISSN 2278 -1412

Securing Multimodal Biometric Data through Watermarking and Steganography

Rakhee Singh Thakur[1], Vimal Shukla[2]

[1] *MTech Scholar, Department of Cyber Security, Kailash Narayan Patidar College of Science and Technology, Bhopal, rakheesinghthakur2001@gmail.com, India;*
[2,] *H.O.D, Department of Cyber Security, Kailash Narayan Patidar College of Science and Technology, Bhopal,vimalshukla.cse@gmail.com, India;*

Abstract— *Data security is main concern in digital technology, especially when data transfer and store. Many times data is sensitive and may be impossible to recover if lost, counterfeited, or hacked. Here, present an approach for hiding biometric data, which utilizes a combination of digital watermarking and steganography. The combination of these techniques enables the system to handle many issues associated with storing and transferring raw biometric data. In [1] proposes is a multilayer framework that first, encodes eigen-features extracted from raw face images, into a fingerprint image. Sequentially, each watermarked fingerprint image is encoded within an arbitrary host image unrelated to biometrics or forensics, securing the image for transfer. The contributions of this work are as follows: developed an application of biometric watermarking face eigen features into fingerprint images that are usable to provide authentication. In proposed work we are design blind watermark with stegonography.*

.

I. Introduction

Biometric confirmation systems have inherent advantage above earliest personal identification techniques [2]. However, there are several essential problems in planning a practical biometric system. These problems are generally characterised by precision, calculation speed, cost, safety, scalability and real time performance. The word steganography is of Greek based and means that "cover, or concealed writing" Steganographyis the art and science of writing hidden messages in such the way that nobody apart from the sender and supposed recipient even realizes there's a hidden message. Generally, a steganographic message can appear to be something else: an image, an article, a shopping list, or another message. A steganographic message (the plaintext) is commonly 1st encrypted by some ancient means that, manufacturing a cipher text. Digital image steganography system may be a stand-alone application that mixes steganography and encryption to boost the confidentiality of supposed message. The user's supposed message is 1st encrypted to make unintelligible cipher text. Then the cipher text are going to be hidden within a picture get into such the way as to minimize the perceived loss in quality. The recipient of the image is ready to retrieve the hidden message back from the image with this technique. Typically, image watermarking is perform by means of discrete wave transform (DWT) as a result of DWT preserves frequency data in stable type and permits smart localization each in time and spatial frequency domain .However, one among the major drawbacks of DWT is that the transformation doesn't give shift invariability as a result of the down sampling of its bands. As biometry becomes additional prevalent in everyday life, there's much interest in making sure that the information associated with the identification of every individual is as secure as potential. database architectures have long been primarily designed to store biometric information in centralized locations [1][2]. However, having a single location or centralized database holding sensitive biometric data can become a treasure chest for fraudulent individuals. One way for an individual to gain unauthorized access to biometric data is during the transfer of data from one location to another. the encryption of biometric data is considered to be effective to a certain degree [4], it is typically reliant
on the secret key that is used depending on the encryption system. However, if the secret key is hacked or leaked, further methods of protecting and securing the data must be in place. Another way of securing data is to hide information within a related

piece of data, such as hiding a face image within the fingerprint of the same subject. This allows for multiple biometric data (multimodal) of one subject to be transferred or moved at a single time. However, if data is properly decrypted and hacked during its transfer, the perpetrator does not need to be aware that the content of the data is sensitive. Therefore, an extra step of prevention must be taken to ensure that if a hacker intercepts data, its immediate visual content appears trifling and of no value. The use of steganography can further ensure the security of biometric data. Steganography is the practice of hiding data in another unrelated piece of information. This helps strengthen data security by masking the truly sensitive information within other data that is irrelevant to the task at hand. As an example, a fingerprint image can be hidden into an image of a sailboat. Therefore, if a hacker obtains this data, he/she can only visually see an image of a sailboat, instead of the sensitive fingerprint information that is hidden within. Using all of these techniques together can significantly increase the security of biometrics data when they need to be exchanged among different parties, e.g. when being transferred from one location to another. bit-stream and are repeatedly embedded into the fingerprint image using an encoding technique designed specifically for biometric watermarking [6]. After this, we utilize a steganography technique to hide the resultant fingerprint/face watermarked data into an arbitrary image of no relevance to biometrics or forensics. During the steganography step, the watermarked fingerprint/face image is converted into a binary stream and the maximum pixel intensity is used to determine the number of bits necessary for steganography. The embedding locations are randomly set across all 3 color channels of the arbitrary image.

II. Literature Survay

Cameron Whitelam et al [1] "Securing Multimodal Biometric Data through Watermarking and Steganography" In this topic, Author have provided an outline to a multilayered watermarking and steganography approach to securing multimodal biometrics. First, eigen-features are watermarked within a corresponding fingerprint image using a watermarking technique specifically for grayscale images. Combining numerous biometric traits for data transfer is essential when multimodal verification is necessary. Secondly, the resultant watermarked image is embedded into an arbitrary image with no relevance to biometrics whatsoever. This provides an extra layer of security to the user if the data is compromised, considering the responsible party will have no indication that biometric data is present. Finally, a multi-layered security framework was described using public key encryption to further ensure the security and authenticity of the biometric data during transfer. It has been shown that the eigen-features and fingerprint image can be successfully embedded into their respective images with little to no visual perception and high bit extraction rates.The authors recognize that there is still a lot of work to be done on this topic and offer this work as a proof of concept. One of the areas that the authors would like to expand their work is to study the effects that certain levels of image compression have on the extraction process. Secondly, the authors would like to perform actual face and fingerprint verification studies after the extraction process. This will stand as another metric to show the accuracy of the extraction rates, as well as to simulate a full biometric verification system. Finally, the authors would like to experiment with different fingerprint feature extractors to alter the (i; j) term to determine its effect on biometric verification. This future work is important to fully show the potential that a multi-layered watermarking and steganography approach has on securing multimodal biometric data.

Mayank Vatsa et al [2]"Feature based RDWT watermarking for multimodal biometric system" This represent 3 level RDWT biometric water marking algorithm to embed the voice biometric MFC coefficients in color face image of the same individual for increased robustness, security and accuracy. Phase congruency model is used to calculate the embedding locations which preserves the facial features from being watermarked and ensure that the face recognition accuracy is not compromise. Using Redundant Discrete Wavelet Transform, the voice coefficients are embedded into the color face image at the same time as preserving the facial features. The robustness of the watermarking algorithm is evaluated by doing comparison of the recognition accuracies of face, voice, and multimodal biometric algorithms. Experimental outcome shows that the projected biometric water marking algorithm is resilient to different signal processing attacks with reduce of 0–1.3% in multimodal biometric verification accuracy. Further, evaluation using different appearance and characteristic based face recognition algorithms demonstrate that the proposed watermarking algorithm does not alter the biometric information required for recognition.

The projected watermarking algorithm uses adaptive user-define watermarking parameter for improved performance. Using face, voice and multimodal recognition algorithms, and statistical evaluation, Author illustrate that the projected RDWT watermarking algorithm is robust to unlike frequency and geometric attacks, and provide the multimodal biometric authentication accuracy of 94%.

Nick Bartlow [3] "Protecting Iris Images through Asymmetric Digital Watermarking" The arrangement of the technique employed by the projected system offers various smart features and advantages. It affords multiple levels of confirmation through cryptography, by watermarking, and through multimodal biometric authentication. By watermarking a attribute vector from a behavioral biometric, author attain both added protection after decryption and a degree of biometric change ability both at the feature vector level and raw image level. The structure offers multiple levels of forgery finding with a arrangement of watermarks and file hashing. Essentially the profile can be considered entirely breakable as it can identify alteration of a particular bit through cryptographic hash comparisons. Additionally, the arrangement offers non-repudiation of basis through PKI and origin tracking through watermarking. Lastly, the cost of compromise is less than systems watermarking biometric data with physical biometric template, as they effectively double the risk connected with compromised profile I tokens.

Anil K. Jain[4] "Hiding Biometric Data" The ability of biometrics-based personal recognition method to discriminate between an authorized person and an fake who fraudulently acquire the contact privilege of an authorized person is one of the core reasons for their fame compared to traditional recognition techniques. However, the protection and integrity of the biometric data itself are significant issue. Encryption, watermarking, and steganography are some possible technique to make safe biometric data. In this, two applications of watermarking to protect that data are presented. In accumulation to watermarking, encryption can also be used to further increase the safety of biometric data. The first application is related to rising the security of biometric data swap, which is based on steganography. In the second purpose, author embeds facial information in finger print images. In this application, the data is hidden in a way that the features that are used in fingerprint identical are not significantly changed at some point in encoding/decoding.
As a result, the verification accuracy based on decoded watermarked images is extremely similar to that with original images. The planned methods utilize several properties of the human being visual system to keep the visibility of the changes made to the host image low. Author is currently working on increasing the data hiding capacity of the host images. Another topic for future research is to examine how dissimilar (e.g., robust and fragile) watermarking schemes can be combined.

Abbas Cheddad [5]"Biometric Inspired Digital Image Steganography " Digital Steganography could be a fascinating scientific space that falls under the umbrella of security systems. Author given during this work some background discussions on algorithms of Steganography deployed in digital imaging. The rising techniques like DCT, DWT and adaptive Steganography aren't an easy target for attacks, especially when the hidden message is small. that's as a result of they alter bits within the transform domain, therefore image distortion is kept to a minimum. usually these strategies tend to possess a lower payload compared to spatial domain algorithms.
In short there has forever been a trade off between robustness and payload. Our projected framework, Steganoflage, is predicated on edge embedding within the DWT domain victimisation skin tone detection in RGB sequential image files. Author chose to use the latter to compensate for the restricted capability that edge embedding techniques demonstrate. Auhtor use the particular components of the image when hiding a message. This leads to many exciting and difficult future analysis issues.
ChunLei Li et al [6]"Protecting Biometric Templates Using Authentication Watermarking "A novel system for defending biometric templates using salient region-based authentication watermarking is proposed in this . Firstly, a novel hierarchical authentication watermarking scheme is proposed, demonstrate a good performance on tamper detection even when the tamper ratio is up to 0.7. Secondly, a self-recovery algorithm of biometric template is presented found on the alike method, the improved PCA coefficients can also be used for recognition system, and the reconstruct face be capable of be use as a instant source of validity. Finally, the effect of watermark for the biometric image is shown, providing guidance for biometric watermarking algorithm. Experimental results shows that the proposed hierarchical verification watermarking

system has better tamper localization, and can efficiently recover the tampered biometric features at the same time as keeping ”recognizing quality” to some extent.

III. Method

A inspiration for the use of watermarking and stagnography techniques in biometric systems has been the need to provide increased security to the biometrics data themselves. Proposed introduce an application of wavelet based watermarking method to hide the fingerprint minutiae data in images. The application provides a high security to both hidden data (i.e. fingerprint minutiae) that to be transmit and the host image. The original unmarked image is not required to extract the minutiae data. Data watermarking is using wavelet packet decomposition. Along this proposed stagnography apply for more security of the data. Steganography and watermarking bring a variety of very important techniques how to hide significant information in an undetectable or/and irremovable way in audio and video data. Watermarking and Steganography are main parts of the fast developing area of information hiding. The utilize of steganography can further ensure the security of biometric data. Steganography is the practice of hiding data in another unrelated piece of information. This helps strengthen data security by masking the truly sensitive information within other data that is irrelevant to the task at hand.

Stegonography:-A common model of a cryptographic system has already emerged.

Watermarking:- In Watermarking Systems Figure 2 shows the basic scheme of the watermarks embedding system.

Inputs to the design are the watermark, the cover data and an optional public or secret key. output is watermarked data. The key is use to enforce security. Figure 3 shows the basic scheme for watermark recovery scheme

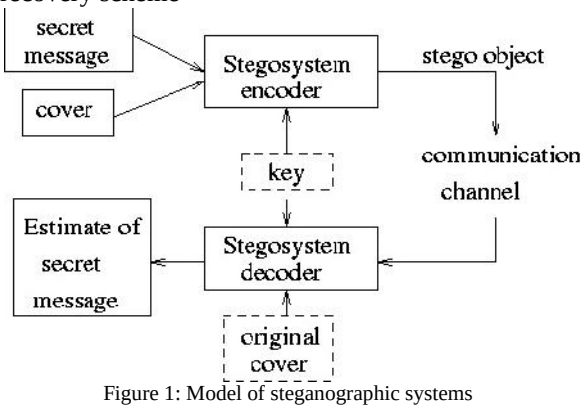

Figure 1: Model of steganographic systems

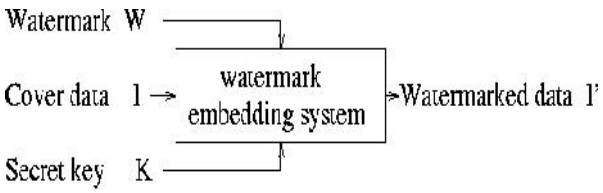

Figure 2: Watermark embedding scheme

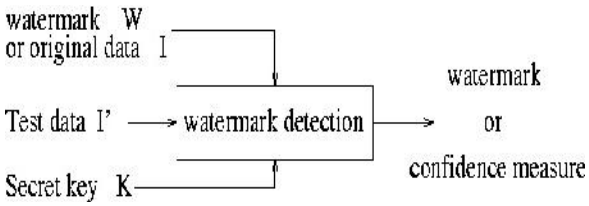

Figure 3: Watermark recovery scheme

input to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data or/and the original watermark. The output is the recovered watermarked W or only some type of confidence measure indicating how probably it is for the given watermark at the input to be present in the data under examination.

Private (non-blind) watermarking systems need for removal/detection the original cover-data.

• Type I system use the original cover-data to extract the watermark from stego-data and use real cover-data to determine where the watermark is.

• Type II systems need a copy of the embedded watermark for elimination and just defer a yes/no answer to the question conditions stego-data contain a watermark. Semi-private (semi-blind) watermarking do not use the real cover-data for recognition, but tries to answer the similar question. (Potential function of blind and semi-blind watermarking is for proof in court possession,)

Public (blind) watermarking - neither cover-data nor implanted watermarks are necessary for removal - this is not an easy problem.

IV. Conclusion

In this paper, we have provided an outline to a multilayered watermarking and steganography approach to securing multimodal biometrics. First, eigen-features are watermarked within a corresponding fingerprint image using a watermarking technique specifically for grayscale images. Combining numerous biometric traits for data transfer is essential when multimodal verification is necessary. Secondly, the resultant watermarked image is embedded into an arbitrary image with no relevance to biometrics whatsoever.

This provides an extra layer of security to the user if the data is compromised, considering the responsible party will have no indication that biometric data is present.

V. Reference

[1] T. Bourlai, L. Messer and J. Kitler. "Face Verification System Architecture Using Smart Cards", In Proc. of 17th International Conference on Pattern Recognition (ICPR), vol. 1, pp. 793-796, Washington D.C., 2004.

[2] T. Bourlai, J. Kittler and K. Messer, "On Design and Optimization of a Face Verification System that is Smart-Card-Based", Journal of Machinge Vision and Applications, Springer, vol. 21, no. 5, pp. 695-711, 2010.

[3] N. Bartlow, N. Kalka, B. Cukic and A. Ross, "Protecting Iris Images through Asymmetric Digital Watermarking," In Proc. of 5th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pp.192-197, Alghero, Italy, 2007.

[4] A. Cavoukian and A. Stoianov. "Biometric encryption," In Encyclopedia of Biometrics. Springer Verlag, 2009.

[5] R. Hunt. "Pki and digital certification infrastructure" In Proc. of Ninth IEEE International Conference on Networks, pp. 234-239, 2001.

[6] A. K. Jain and U. Uludag, "Hiding Biometric Data", IEEE Transaction On Pattern Analysis and Machine Intelligence, vol. 25, no. 11, Washington D.C., 2003.

[7] M. Kutter, F. Jordan, and F. Bossen. "Digital signature of color images using amplitude modulation, In SPIE Proc., vol. 3022, pp. 518-526, 1997.

[8] C.Y. Low, A.B.J. Teoh, C. Tee. "A preliminary study on biometric watermarking for offline handwritten signature," IEEE International Conference on Telecommunications (ICT-MICC), pp.691-696, Penang, Malaysia, 2007.

[9] M. Vatsa, R. Singh, A. Noore, M. Houck, K. Morris, "Robust biometric image watermarking for fingerprint and face template protection," IEICE Electronics Express, vol. 3, no.2, 23-38, 2006.

[10] N.K. Ratha, J.H. Connell, and R.M. Bolle,"A Biometrics-Based Secure Authentication System," Proc. IEEE Workshop Automatic Identification Advanced Technologies, pp. 70-73, Oct. 1999.

[11] B. Gunsel, U. Uludag, and A.M. Tekalp, "Robust Watermarking of Fingerprint Images," Elsevier Pattern Recognition in Information System, vol. 35, no. 12, pp. 2739-2747, Dec. 2002.

[12] A. Georghiades, P. Belhumeur, and D. Kriegman, "From Few toMany: Illumination Cone Models for Face Recognition under Variable Lighting and Pose," IEEE Transaction On Pattern Analysis and Machine Intelligence, vol. 23, pp. 643-660, 2001.

[13] R. Cappelli, M. Ferrara, A. Franco, D. Maltoni, "Fingerprint Verification Competition 2006," Biometric Technology Today, vol. 15, no. 7-8, pp 7-9,July-August 2007.