International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

Distance-Based security data transmission in Biometric-Based Encryption

Mounika Malaga [1], Ravuri Venkata Kiran Kumar [2]
[1] PG Scholar, Dept of ECE, Rise Krishna Sai Gandhi Group of Institutions, Ongole, AP, India.
[2]Associate Professor, Dept of ECE, Rise Krishna Sai Gandhi Group of Institutions, Ongole, AP, India.

Abstract:

Crypto-biometric system model introduces a new encryption notion called distance-based encryption (DBE) Biometrics in identity-based encryption. In this notion, a cipher text encrypted with a vector and a threshold value can be decrypted with a private key of another vector, if and only if the distance between these two vectors is less than or equal to the threshold value. The adopted distance measurement is called Mahalanob is distance, which is a generalization of Euclidean distance. The most important of this new encryption notion is to incorporate biometric identities, such as iris, finger and face. this method, usually the input biometric identity associated with a private key will not be exactly the same as the input biometric identity in the encryption phase, even though they are from the same user. And it shows how to construct generically and efficiently using DBE with reasonable size of private keys and cipher texts. Also proposed a new DBE scheme with the shortest private keys are build. In this encryption efficiently using RSA algorithm

1 Introduction

There has been recent interest about the challenge of generating cryptographic keys from biometric inputs. The primary difficulty in generating a strong key from a biometric input is that the measured value of the a biometric can change slightly upon each sampling. This effect can be explained by differences in sampling devices, environmental noise, or small changes in the human trait itself. This inherent non-determinism makes it difficult to extract a cryptographic key from a biometric input. Recent work has produced techniques to derive cryptographic keys from biometric inputs for symmetric key applications. For example, Monrose et al. [12, 11, 10] develop techniques to extract secrets from keyboard typing dynamics and later voice prints by using a form of error-tolerant secret sharing. Other work by Davida et al. [4] and Juels and Wattenberg [7] use error-correcting codes to compensate for the noise in the biometric input. These techniques are useful for symmetric key cryptography applications such as password authentication and symmetric

key encryption. However, there does not seem to be a clear way to move these techniques into the realm of public key cryptography. In particular the work above seems does not fit into the paradigm of Identity Based Encryption. We propose a new type of Identity Based Encryption that we call Fuzzy Identity Based Encryption. In a Fuzzy Identity Based encryption scheme a user with secret key for the identity id is able to decrypt a ciphertext encrypted with the public key id0 if and only if id and id0 are within a certain distance of each other as judged by some metric. For the remainder of this paper we view identities as n bit vectors and use the Hamming distance between them as the metric of distance. However, a Fuzzy Identity Based Encryption scheme could be built using some other metric.

1.1 Our Contributions

We introduce Euclidean Distance based Encryption (EDE). In this encryption notion, a private key of vector ~y can decrypt a ciphertext encrypted with another vector ~x and a threshold value t, if and only if the Euclidean distance between ~x and ~y is less than or equal to t. The primary motivation of this work is to bride the gap between biometric based encryption and pattern recognition. In this poster, we propose this encryption notion and study its construction. The adopted Euclidean distance measurement is called weighted squared Euclidean distance, which is a generalization of (squared) Euclidean distance. We show how to generically and efficiently construct an EDE from an inner-product encryption (IPE) with reasonable size of private keys and ciphertexts. Given any integer k0 defined by the system generator, each EDE key has k0 + 1 numbers of IPE keys and each EDE ciphertext has d t k0 e numbers of IPE ciphertexts. A proper k0 can be selected to balance the size between private keys and ciphertexts. We also propose a new IPE scheme equipped with a specific characteristic to build EDE, namely the need for a short private key. The private key of our IPE scheme comprises of two group elements only, compared to the best efficient IPE scheme in the literature with nine group elements [3]. The EDE instantiation from our IPE will therefore save more than 75% secure memory for private key storage. We prove the security of our IPE scheme with payload security in the selective security model under the Decision Bilinear Diffie-Hellman assumption.

2.LITERATURE SURVEY

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

Watermark Scheme

A watermark should be embedded in such a way that it remains detectable as long as the perceptual quality of the digital content stays at an acceptable level .In general, any watermarking system consists of following parts:Watermark, Carrier, Encoder,Decoder.The conceptual model of the watermarking system is explained in figure 1 . Original image depicts the carrier which needs protection. The watermark encoder embeds the watermark in to the cover image. The watermark can be a pseudo-random number or binary sequence. The optional key is used to enhance the security of the system. Decoder estimates the watermark from the received image with the help of key and original image if required. Watermarked image is subjected to various forms of manipulations on communication channel.

Watermarking schemes can be classified based on the presence or absence of original contentat the time of watermark detection.

(i) Non-blind scheme: It requires presence of original content during watermark detection.

(ii) Blind scheme: It does not require the presence of original content while decoding thewatermark.

In the early days non-blind watermarking schemes were popular as they were more robust thanblind schemes. It is due to the fact that in watermarking model, original content is treated as anoise source to watermark, which is the signal of interest. Presence of original content at thereceiver nullifies the effect of this noise. However, non-blind schemes suffer from two distinctdisadvantages.

(i) Security compromise: Non-blind detection does not guarantee unequivocal claims of ownership by the content creator. Attacker can easily fool the system and even worst, may claimthe ownership by inserting another watermark in the content.

(ii) Practical application constraints: It is not possible to ensure presence of original contentduring detection for every watermarking application. For e.g., copy protection in DVD. With the development in watermarking research, blind schemes are matching the performance criteria of non-blind schemes. Hence state-of-art watermarking system offers blind detection, which is the case with this work as well.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

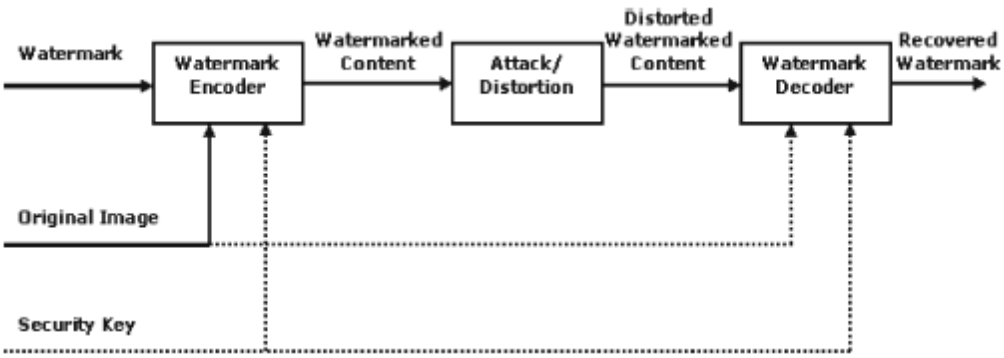


Figure 1.A typical watermarking system.

Watermarking Systems

In this scheme, an entropy masking model has been applied on the host image for the texture segmentation. Moreover, the local luminance and textures of the host image are considered for watermark embedding procedure to increase the robustness of the watermarking scheme. In contrast to all existing SVD-based watermarking systems that have been designed to embed visual watermarks, our system uses a pseudo-random sequence as a watermark. We have tested the performance of our method using a wide variety of image processing attacks on different test images. A comparison is made between the results of our proposed algorithm with those of a wavelet-based method to demonstrate the superior performance of our algorithm.

An Effective Wavelet-Based Watermarking Scheme Using Human

On behalf of the content owners and distributors, copyright protection and content authentication of digital content has developed into a grave problem. This issue can be resolved by the solution offered by the Digital watermarking. In recent times, Digital watermarking has seen rapid escalation. Ownership protection, authentication, and content integrity verification of intellectual property in digital form have comprehensively utilized watermarking, of late. The process of embedding data into multimedia elements such as images, audios and videos is defined as watermarking. The detection or extraction of this embedded data from the multimedia offers the proof of ownership or other purposes.

Diverse ways can be employed to find the different classifications of watermarking and watermarking techniques. Generally, the literature available deals with two classes of

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

digital watermarks namely the visible and invisible watermarks. In visible watermarks, the ownership of the image is illustrated by the distinctive unique visible message or a company logo and in the invisible watermarks, the invisibly watermarked digital content and the original image are extremely alike when envisaged. The intent of the design of the major accessible invisible watermarking schemes is to offer either the copyright protection or content authentication. Robust and fragile watermarks are the two extensive categories of the invisible watermarks, the former principally intends at copyright protection where the need for high resistance against numerous signal processing operations is signified by the term robust. In contrast, content authentication is the primary objective of the latter. In addition, non-blind, semi-blind and blind methods are the divisions of watermarking. In non-blind methods, the original image itself are employed for the extraction of watermark, while the certain characteristics of the original image are engaged by the semi-blind methods, whereas the detection process in the blind methods do not necessitate the original image.

A good watermarking scheme should be robust enough to defend against attacks while being invisible such that the dissimilarity between the watermarked image and the host image should not be distinguishable by the human eyes.

A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT

The watermark is a signal embedded into the host media to be protected, such as an image or audio or video.It contains useful certifiable information for the owner of the host media, such as producer's name, company logo, etc; the watermark can be detected or extracted later to make an assertion about the host media . For this aim, digital watermarking techniques are developing and their number is growing, searching all for the equilibrium between three criteria: data hiding capacity, imperceptibility, and robustness, depending on the image domain representation.

The choice of a domain lies mainly on robustness criteria required relating to specific data manipulations or malicious attacks. Between these domains the spatial presentation is robust against geometrical attacks. In the other, hand its restrictions dissuades its use because of the poor capacity of data embedding with respect to the imperceptibility condition. In order to further performance improvements in DWT based digital image watermarking

algorithms could be obtained by jointing DWT with DCT.

Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication

The proposed algorithm embeds a perceptually recognizable binary pattern, such as owner's logotype. Firstly the video sequences are segmented by each scene, and then the binary watermark pattern is embedded into Discrete Wavelet Transform (DWT) domain of the randomly selected scene blocks. To increase the security of the proposed scheme, the biary watermark pattern is mapped to a noise like binary pattern using a chaotic mixing method, before its embedding. Simulation results show the watermark imperceptibility and robustness against several attacks, such as noise contamination, frame dropping, frame averaging and frame swapping; the evaluation results also show that the extracted watermark pattern is sufficiently clear, although the watermarked video sequence may suffered several attacks.

Digital Video Watermarking in DWT Domain Using Chaotic Mixtures

Various comprehensive investigations on the existing watermarking technologies have been accomplished. And it has been discerned that none of the recent watermarking schemes can resist all sorts of attacks. With this outcome, this paper proposes a robust scheme for digital video watermarking based on scrambling & then embedding the watermark into different parts of the source video according to its scene change. Certain watermarking schemes of each class have been preferred for enactment and various tests are accomplished to relate their robustness. Literature review reveals that watermarking schemes can be crudely divided into two classes: spatial domain, and transformed domain. Some of the spatial domain techniques discussed are: Least significant bit (LSB) based watermarking scheme: The most straightforward method of watermark embedding would be to embed the watermark into the least significant bits of the cover object. 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 1, fully defeating the watermark with negligible impact on the cover object. Threshold based correlation watermarking scheme: G. Langelaar,has discussed the threshold and non threshold based watermarking scheme. Direct sequence watermark using m-frame: B. Mobasseri has applied a direct sequence

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

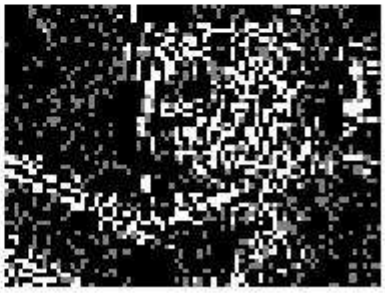
spread spectrum model to the watermarking of digital video. The watermarked video is robust to video editing attempts such as sub-sampling, frame reordering.

3. RESULTS

The experimental results of the proposed digital video watermarking scheme using discrete wavelet transform are presented. The watermarked video sequences possess superior Peak Signal to Noise Ratio (PSNR) and visual quality for grayscale watermark images.

The output acquired from the proposed video watermarking scheme has been evaluated by PSNR and NC (Normalized Correlation).

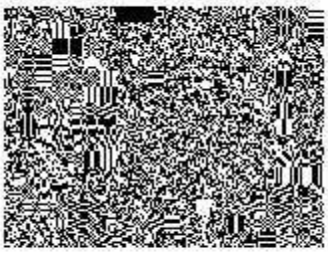


e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

watermark image

Bit plane 1



Bit plane 2

Bit plane 3

Bit plane 4

Bit plane 5

Bit plane 6

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 2
February 2019

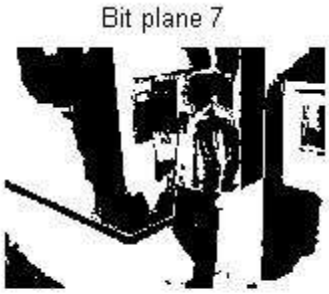


Fig.1.Watermarked Image

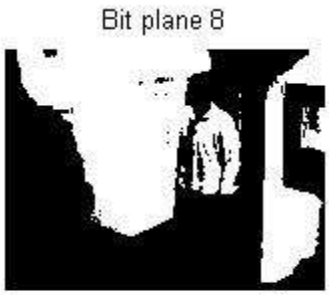


Fig.2.watermarked Video

Fig.3.Watermarked Frame

3.Concusion

In the present world, the information sharing via public communication channel is not yet studied and focused effectively. Identity-Based Encryption (IBE) is a particular public key encryption which allows users to use their identity information as public keys. The identity information could be created in a different combination order in encryption and key generation, Such that the decryptor has to apply a new private key for it. Biometric traits such as iris, fingerprint, face, and hand gementory can be also used to represent the identities of users due to their unique biological features. The Iris identification is save the private key storage. In this works studied about

the distance based encryption and identity based encryption schemes. This schemes aims to transfer the message in secured communication systems.

References

[1] F. Guo, W. Susilo, and Y. Mu, "POSTER: Euclidean distance based encryption: How to embed fuzziness in biometric based encryption," in Proc. ACM Conf. Comput. Commun.Secur., 2014, pp. 1430–1432.

[2] T. Kanade, "Picture processing system by computer complex and recog-nition of human faces," Ph.D. dissertation, Dept. Inf. Sci., Kyoto Univ., Kyoto, Japan, 1973.

[3] R. Brunelli and T. Poggio, "Face recognition: Features versus templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 15, no. 10, pp. 1042–1052, Oct. 1993.

[4] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching,"IEEE Trans. Image Process., vol. 9, no. 5, pp. 846–859, May 2000. [5] H. Moon and P. J. Phillips, "Computational and performance aspects of PCA-based face-recognition lgorithms,"Perception, vol. 30, no. 3, pp. 303–322, 2001

Author's Profile:

MOUNIKA MALAGA has received her B.Tech Degree in Electronic Communication Engineering from Pace Institute of Technology and Sciences affiliated to JNTU Kakinada in 2015 and pursuing M.Tech degree in DECS in Rise Krishna Sai Gandhi Group of Institutions, Ongole affiliated to JNTU Kakinada in 2017, AP, India.

RAVURI VENKATA KIRAN KUMAR has received his B.Tech in Electronics & Communications Engineering from Malineni Lakshmaiah College of Engineering & Technology, affiliated to JNTU Hyderabad in 2006 and M.Tech degree in DECS from Samuel George college of Engineering affiliated to JNTU Kakinada in 2012.He is dedicated to teaching field from last 12 Years. He has guided 12 P.G students.His research areas included Signal Processing. At present he is working as Associate professor in Rise Krishna Sai Gandhi Group of Institutions, Ongole, affiliated to JNTU Kakinada in AP, India.