ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Multimodal Biometric Watermarking Techniques: A Review

C.Karthikeyan[1], D.Selvamani[2]

Assistant professor, Dept. of ECE, Einstein Engineering College, Tirunelveli, Tamilnadu, India[1]

PG Student, Dept. of ECE, Einstein Engineering College, Tirunelveli, Tamilnadu, India[2]

ABSTRACT: Multimodal biometric systems are being gradually deployed in much large scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to unibiometric systems. A number of watermarking algorithms have been proposed, they have limited real-world applicability due to the balance between credit performance and security of the template. In this paper, a universal evaluation of the main literature related to the Bio watermarking is presented together with classification by using a variety of techniques.

KEYWORDS*:*Multimodal biometric, UnibiometricWatermarking, Security.

I.INTRODUCTION

We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital sources and collections, web publishing) has developed many fold. Meanwhile reproduction a digital data is very easy and loose besides so, issues like, protection of moralities of the content and verifying ownership, arises. Digital watermarking is a technique and a tool to copyright laws for digital data. The field of watermark is that it remains complete to the refuge work even if it is copied. So to prove possession or copyrights of data watermark is extracted and verified. It is very difficult for criminals to eliminate or change watermark. As such the real holder can always have his data safe and secure.

Biometric identification systems have recently gained considerable attention from the research community, since these systems have been used in various commercial applications such as surveillance and access control against potential imposters. Now a day, multimodality is a new and rapidly developing subject of research in the field of biometrics. Multimodal biometric systems are a type of pattern recognition systems, which identifies an individual on the basis of physiological or behavioural characteristics, like that fingerprint, face, iris, retina, palm, voice, and vein. In order to recognize individuals, multi-biometric systems use more than one biometric trait. These systems provide higher recognition rate as compared to uni-biometric systems that relay on only one biometric trait.The main aim of this paper to study different watermarking techniques.

II.REVIEW OF LITERATURE

Mayankvasta,RichaSingh,P.Mitra et al .[1] explains digital watermarking based Secure multimodal biometric system .In this paper, dual levels of security are proposed for concurrently authenticating any individual and guarding the biometric templates. In these systems uses two watermarking algorithms namely Modified Correlation based algorithm and Modified 2D Discrete Cosine Transform based algorithm. This watermarking algorithm provides high security. Once the system is affected by the attacks biometric templates will not be replaced.

Mayankvasta, Richa Singh et al. describes the Feature based RDWT Watermarking for multimodal biometric system [2] This paper presents a 3-level RDWT biometric watermarking algorithm to embed the vocal sound biometric MFCcoefficients in a colour face image of the same individual for increased robustness, security and accuracy. Phase congruency model is used to compute the embedding locations which conserves the facial features from being watermarked and ensures that the face recognition accuracy is not compromised. This watermarking algorithm uses adaptive user-specific watermarking parameters for improved performance. Using face, speech and multimodal

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

recognition algorithms, and statistical evaluation, RDWT watermarking algorithm is robust to different frequency and geometric attacks

The RDWT watermarking algorithm first computes the embedding capacity and location in the face image using edge and corner phase congruency method. Embedding and extraction of voice data is based on Redundant Discrete Wavelet Transformation. The performance of the watermarking algorithm is validated using face, voice and multimodal authentication algorithms. The proposed watermark embedding and extraction algorithm does not affect the quality of the original face image or the recognition performance. In addition, the algorithm is robust and resistant to common attacks and computational work is complex.

Won-ayumkim,Heungkyu lee in paper titled Multimodal biometric image watermarking using two stage integrity verification[3].This paper, gives multimodal biometric image watermarking scheme through a two-stage integrity verification method using the secreted thumbnail feature vectors for safe authentication of multimodal biometrics data, face and fingerprint, respectively. It is essentially shade and spread spectrum-based robust watermarking method. This method enables to detect a tampered region by controlling watermark embedding forte to meet the requirement of predefined watermark extraction threshold. The vital idea is that the thumbnail feature vectors of a face image as a watermark pattern are used by embedding into a fingerprint image in order to check the reliability of respective biometric data. The first stage of honor proof for a fingerprint image is done by determining the validity of extracted thumbnail patterns. The stage of integrity verification for a face image is done by one-to-one matching between the thumbnail feature vectors extracted from a face image and the thumbnail one of the received face image. This paper, clarifies the spatial domain-based robust biometric image watermarking technique using dual-step integrity verification method which identifies the integrity of biometric data using secreted thumbnail feature vectors for security guarantee. Here in, fingerprints and face biometric data are used for multimodal confirmation scheme. Two biometric data are captured and transmitted into the biometric authentication system. The thumbnail feature vectors of the face image are only watermarked into the fingerprint image as a cover water- mark for data hiding before transmitting. Then, at the biometric authentication system, the integrity of water- marked fingerprint image is checked first by checking the validity of thumbnail feature vectors (watermark) extracted using a predefined watermarked extraction threshold. Secondly, the thumbnail feature vectors extracted from a watermarked fingerprint image is related to the thumbnail one of the transmitted original face image to recognize the integrity of the face image. From the two-stage integrity identification method, the final decision-making is completed.

To embed the watermark using biometric features or general identifiable watermark design, spatial domain or transform domain watermarking scheme such as fast Fourier transform (FFT), discrete wavelet transform(DWT),discrete cosine transform (DCT) , and Radon transform can be applied. It is well famous that the transform domain watermarking technique has robustness and higher performance than the spatial domain watermarking scheme. However, if the robustness is guaranteed, spatial domain watermarking scheme is better than frequency domain one because it is simple and fast.

Hung- Hsu Tsai, Chi-ChihLiu describes Wavelet-based image watermarking with visibility range estimation based on HVS and neural networks [4], this work proposes a wavelet-based image watermarking (WIW) technique, based on the human visible system (HVS) model and neural networks, for image patent protection. A characteristic of the HVS, which is called the just noticeable difference (JND) profile, is employed in the watermark embedding to enhance the silence of the technique. First, derive the acceptable visibility ranges of the JND thresholds for all coefficients of a wavelet-transformed image. The WIW technique exploits the ranges to compute the adaptive metiers to be covered in the wavelet coefficients while embedding watermarks. An artificial neural network (ANN) is then used to remember the affairs between the original wavelet coefficients and its watermark version. Therefore, the trained ANN is used for estimating the watermark without the original image. Then the computer simulations validate that both transparency and strength of the WIW technique are larger to that of other methods. Here the robustness is less, then it having a less embedding capacity.

Sengul Dogan, TurkerTuncer, EnginAvci et al. [5]A robust colour image watermarking with Singular Value Decomposition method, The performance of a watermarking method based on Singular Value Decomposition (SVD) has been enhanced for colour image in this paper. One of the common methods used for hiding data on image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

documents is Singular Value Decomposition method which used in the frequency domain. In Singular Value Decomposition based watermarking techniques, watermark embedding can be usually attained by changing the least significant bits of the singular value matrix. It specifies the precise image property but it is not fit for malicious attacks.

Punam Bedi,RoliBansa et al [6] here the authors are presents a Multimodal Biometric Authentication using PSO based Watermarking. This paper presents a robust multimodal biometric image watermarking scheme using Particle Swarm Optimization (PSO). The key idea is to watermark an character's face image with his fingerprint image and data. PSO is used to select best DCT coefficients in the face image for embedding the watermark. The impartial function for PSO is based on the human visual perception skill and ability of the watermarked image to tolerate image processing attacks. Particle Swarm Optimization is a computational method that optimizes a problem by iteratively annoying to improve a applicant solution with regard to a given measure of quality. It is motivated by social comportment of bird flocking or fish schooling. A PSO algorithm maintains a swarm of particles, where each particle represents a possible solution. All particles have suitability values, which are evaluated by the suitability function to be optimized and have speeds which direct the movement of the particles. This system is less robustness, then the system is easily affected by frequency attacks.

Novel Approach for Multimodal Biometric System Using Compressive Sensing Theory based Watermarking Proposed by RohitM.Thanki and KomalR.Borisagar which comprises, compressive sensing theory for generation of measurement features of biometric model of individual and embed into another biometric template of same individual to generate multimodal biometric watermarked image. This watermarked version of biometric image is use for matching with registered biometric templates and if matching is not possible then extracts quantity biometric features from watermarked image and match with second enrolled data of individual. This paper also shows that how improved data storage capacity at system database and protection of multi biometric template over noisy communication channel.

III. CLASSIFICATION OF WATERMARKING SYSTEMS

This section will discuss about the some of the popular watermarking algorithm that are used for multimodal biometric watermarking systems.

1) Modified Correlation based system

This watermarking system uses modified correlation watermarking algorithm. The iris code is watermarked into face image using secret key. Before watermarking the cover image is pre-processed by using pre filtering techniques, the pre-processing increases the high result correlation. The face image act as cover image then iris is a watermark image. The additive pseudo random noise is applied to the biometric templates for watermark embedding. During watermark extraction the iris code extract from watermarked face image using same secret key and then calculate the correlation between noise pattern and watermarked image. If the correlation is greater than a certain threshold value, the watermark is decoded and a single bit is set. The entire image is divided into various blocks and performing the above procedure separately on each blocks even the attacks are present in this systems it gives high probability correct decision for decoding.

2) Modified 2D discrete cosine transform based system

In this system the image is divided into 8×8 blocks and discrete cosine transform of the image is calculated on each blocks of image then find the lowest and highest frequency coefficient components of the image.so the DCT approaches for watermarking systems do not give some forms of attacks.

3) Redundant Discrete Wavelet Transform (RDWT) based watermarking system

Mostly the discrete wavelet transform is used in image watermarking because discrete wavelet transform gives frequency information in stable form and it allow good localization both in time and frequency domain. Conversely The DCT having one of the main demerits is that the transformation does not provide shift invariance because of the down sampling of its band. The shift variance of the DWT leads incorrect extraction of watermarking systems so we need to know the precise locations of where the watermark information is embedded so the small shift variance cause the wavelet coefficient of the input image but The RDWT overcomes the shift variance problem.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

In RDWT biometric watermarking algorithms to make the watermark visible to the human eye. The RDWT watermark embedding and extraction process does not change the biometric features required for recognition. This systems use colour face image as cover image. The fingerprint, iris code, voice data are the watermark image. The face image divided into three channels (red, blue, green) which increase the embedding capacity. The red and blue channels are used to make the watermark imperceptible although the green channel makes the watermark visible.RDWT compute correct locations for hiding the watermark in a face image. The extracted image obtained by using inverse transformation and it is used for verification.

4) Wavelet based watermarking system

In this uses wavelet based watermarking techniques and it is based on the human visible system. The human visible system having the one essential characteristics that is Just Noticeable Profile (JND) which is used for watermark embedding to improve the imperceptibility of the system. First estimate the allowable visibility ranges of the JND threshold for all coefficient of the wavelet transformed image. The system deeds the range to calculate the adaptive strength to be covered in the wavelet coefficient while embedding watermark. Then the system exploits the artificial neural network which is used for remember the relationship between the original wavelet coefficients and its watermark version. During the extraction the trained artificial neural network used to calculate the watermark coefficient without use of the original image. It gives better performance compared to other watermarking systems.

5) Singular value Decomposition based watermarking system

The SVD based algorithms mostly used in image processing and visualization it operates only on a positive matrix. The cover image considered as a matrix then the cover image matrix divided into three sub matrix with singular value decomposition and watermark image added with cover image matrix it having the singular values and it will generate watermarked image. The decomposition technique is applied to the watermarked image. Finally the watermark image decoded from cover image using decomposition method. This system gives the very good image stability and intrinsic algebraic image properties.

6) Particle Swarm Optimization based watermarking system

In particle swarm optimization methods, the cover image divided into different blocks and calculates the best DCT coefficients for watermark embedding. A PSO algorithm maintains a swarm of particles where each particle indicates the optimal solution .This method does not required original image for watermark extraction. The main function of PSO is to reduce the robustness and improves the imperceptibility of the systems. After extraction the extracted image is good quality even if the attacks are present in the systems.

7) Compressive sensing theory based watermarking system

This systems generate the measurement vector about the watermark templates by using the image transformation and measurement matrix and the measurement vectors embedded into the cover image.so the security is very difficult because it is very difficult to recover the secure biometric templates from measurement vector without Knowledge of original measurement matrix and image transformation.

IV. CONCLUSION

Multimodal biometric watermarking is a growing research area that has received great benefit from the research community over the past era. In this paper, an inclusive survey of the important researches and techniques existing for multimodal watermarking has been inspected. Here, existing researches that are robust against attacks are investigated. An introduction about the multimodal watermarking has been presented and the existing researches are ordered according to the techniques implemented. These review overlays the way to the potential researchers to know about the various techniques available for Biometric watermarking.

REFERENCES

[1]MayankVatsa, Richa Singh, P. Mitra, AfzelNoore.,"Digital Watermarking based Secure Multimodal Biometric System",2004 IEEE lntemational Conference on Systems, Man and Cybernetics.

[2]MayankVasta,Richa Singh, AfzelNoore.,"Feature based RDWT watermarking for multimodal biometric system",ELSEVIER,image and vision computing 27(2009) 293-304.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

[3]Won-gyumKim,HeungKyuLee.,"Multimodal biometric image watermarking using two stage integrity verification",ELSEVIER,signal processing 89(2009),2385-2399.
[4]Hung-HsuTsai,Chi-ChihLiu., "Wavelet based image watermarking with visibility range estimation based on HVS and neural networks",ELSEVIER,pattern recognition 44(2011).751-763.
[5]sengulDogan ,TurkerTuncer,EnginAvci,ArifGulten.,"A robust color image watermarking with singular value decomposition method",ELSEVIER,advances in engineering software 42(2001) 336-346.
[6]PunamBedi, RoliBansal, PritiSehgal.,"Multimodal Biometric Authentication using PSO based Watermarking,",ELSEVIER,Procedia Technology 4 (2012) 612 – 618.
[7]Rohit M. Thanki&Komal R. Borisaga.,"Novel approach for multimodal biometric system using compressive sensing theory based watermarking", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 4, 81-90, Oct 2013.
[8]Asadjaved,Muhammadfasi,tariqbashir.,"A new additive watermarking technique for multimodal biometric identification",journal of Basic and Applied Scientific Research,ISSN 2090-4304,3(7) 935-942.2013.
[9]Chulhanlee,Jaihiekim.,"Cancelable fingerprint templates using minutiae based bit strings,ELSEVIER,journal of network and computer applications 33(2010),236-246.
[10]Mr.AnandKolapkar,Prof.B.B.Gite.,"Secure multimodal Authentication Using Watermarking",Conference,International journal of innovative research in science engineering and technology,ISSN(online):2319-8753, ISSN(print):2347-6710,volume 3,issue 4,april 2014.
[11]Vandana s inamdar and pritirege.,"Dual watermarking technique with multiple biometric watermarks",Indian Academy of Sciencess,vol 39,part 1,february 2014,pp.3-26.