International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 6, Issue 4 (April 2017), PP.27-30

A Survey Paper on Cryptography and Biometrics

S.Uma Mageshwari[1], Dr.R.Santhi[2]
[1]*Research Scholar, R& D Centre, Bharathiar University, Coimbatore.*
[2]*Professor in AVS College of Engineering & Technology, Andhra Pradesh.*

ABSTRACT: In the present scenario, the advancements and development of Information Technology makes the people to depend on various computing devices to do their work efficiently and conveniently. To protect the data from the hackers during transmission, it's best preventing from the unauthorized person access. To achieve this key (Cryptography) and fingerprint, tongue iris…etc (Biometrics) can be used to resolve this problem. This paper is about comparative study on three papers with different algorithms and methods to provide data protection from an intruder. This paper helps you to understand how to provide an enhanced security for data transmission and authentication of a person by integrating features of Cryptography and Biometrics.
Keywords: Cryptography (key), Biometrics (Fingerprint, Tongue) Security, Hackers.

I. INTRODUCTION

Cryptography is a technique used to send data between Sender and Receiver in a secured manner using public key and private key. But still if an intruder identifies the key then the secured transmission of information become unsecured. Moreover, Biometric (physiological and behavioral characteristics) is combined with Cryptographic algorithms for achieving strongest authentication and information security. This paper emphasizes the combination of Cryptography and Biometrics with different approaches for ensuring authentication and permission is granted to access the information after verification.

II. KEY GENERATION ALGORITHMS USING FINGERPRINT IMAGES

Existing Work
In the key generation algorithms [1], key is generated from the biometric data (fingerprint image) and is not stored in the database.

Algorithm [1]
Step 1: Input as Minutiae points.
Step 2: Calculate the Height 'H' by adding (x+y)
Step 3: Plot line from origin (0, 0) to H and Name it as L.
Step 4: Store it in A (array) after sorting of the input points.
Step5: Calculate Val=KL/Sp and Vec= KL%Sp.
Step6: For i=1 to val
For j=1 to Sp
Read each point from Array.
Put '0', if the point is above or on the line otherwise '1' and store it in an array K. **KEY**: ADD Kv + Lk.
Where Mp – Minutiae points, Sp- Size of Mp, KL- Key Length, Kv- Key Vector, Lk- Length of key vector. The above algorithm is dependent of axes. Hence, a slightest change in the fingerprint image it produces a different key.

Improved Version Of Algorithm [1]
Step 1: Find out the relative distances (in mm) such as $M={}^{N}C$ 2.Store in an array A and sort it.
Step 2: G= KL/8, U=M/G, V=M%G
Step 3: Array A divided into groups G and each group with U elements. Apply XOR operation on all the V elements and the output is stored in each group.
Step 4: Use XOR operations in each group by taking mod with a prime number less than (256) and store the results in an array B.
Step 5: Binary form of B store it in K (array), key of length KL.
The above algorithm reduces the complexity of generating crypto keys as well as it works for other physiological characteristics (iris, face, tongue…)

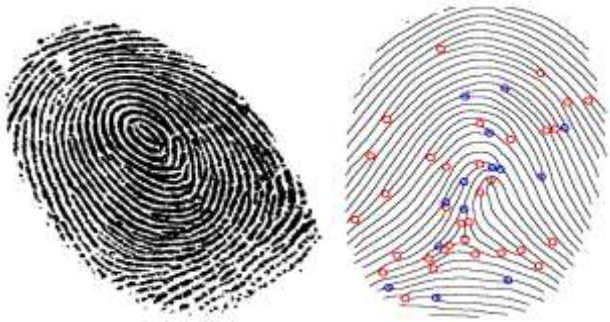

Fig 1: Sample Fingerprint & Minutiae points

III. VISUAL CRYPTOGRAPHY WITH TONGUE AS A BIOMETRIC

In this approach, a Visual Cryptography (VC) the computation[2] is not required in which the security is achieved through sharing of tongue images secretly .Encryption and Decryption is carried out by using Tongue images captured in three views namely,[2]

1. Front View (Texture)
2. Profile View(Shape)
3. Lateral View (Left & Right Movement).

Three different views need to be stored in database for authentication. The incoming tongue images will be compared with the existing templates. [2]To access the data, only an authorized person can do it. An Original binary image I is encrypted in 'n' no. of images such as,

I= S1 XOR S2 XOR S3…..XOR Sk, k<=n

Where k- image, n- no. of noisy images.

[2]In this Scheme, the Pixel P in the original image I is encrypted as two Sub- pixels known as *Shares.* It seems to be difficult to decipher the Secret image I using individual S1….Sk. This methodology can be used in Banking System.

IV. CRYPTO – KEY USING FINGERPRINT IMAGES

In this methodology, both sender and receiver [3] use minutiae points from fingerprint images. The steps involved in this approach are [3]:

1. Feature Extraction (Fingerprint image into Minutiae points)
2. Cancelable Template Generation (Fingerprint templates into cancelable templates)
3. Steganographic Encoding (Cancelable Template shared to other end)
4. Steganographic Decoding(Data Identified Using Key)
5. Merging Templates Ts &Tr (Sender and Receiver Templates joined)
6. Shuffle Key Update(Key is updated in each session)

Every session both sender and receiver generate a unique shuffle key by using fingerprint (minutiae points). The old Shuffle key is destroyed. Thus the unique Cryptographic key is generated with fingerprint-based symmetric Cryptography.

V. CONCLUSION

The authors project their different ideas to achieve security over network and person authentication for safe transaction of information between sender and receiver. [1] The Key Generation algorithm says that the modified algorithm is independent of direction and the loopholes faced in the previous algorithm is resolved by indentifying Centriod C for the given fingerprint image. The computations are needed to find out the Key Length (KL). [2] The Visual Cryptography approach replaces the computations and the key is generated by splitting of original binary image as well as apply XOR operation over it. The encryption and decryption is done with images. Hence, large computations for generating the key is not required as well as the tongue images of different views must be maintained in the database for authentication. [3] In Cryptographic- Key Using Fingerprint data methodology, the various steps mentioned above need to be followed. Both sender and receiver use fingerprint data as an input. The algorithm produces T_S and T_R templates that can be merged to produce a Cryptographic Key (K). Different methodologies have been depicted to ensure secured accessing of information. Thus, combining the Cryptography and Biometrics afford a great impact on authentication and preventing from unauthorized access from an intruder.

REFERENCES

[1]. R. Ranjan, Sanjay Kumar Singh," Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems", IEEE International Advance Computing Conference (IACC) 2013 3rd, 978-1-4673-4529-3/12

[2]. Sowmya Suryadevra, Rohaia Naaz, Shwe, Shuchita Kapoor, Anand Sharma, "Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System", International Conference on Computer & Communication Technology (ICCCT) – 2011, 978-1-4577-1386-611.

[3]. Subhas Barman, Debasis Samanta, Samiran Chattopadhyay,"Barman et al. EURASIP Journal on Information Security (Springer Open Journal) 2015, DOI 10.1186/s13635-015-0020-1.

[4]. SVK Gaddam, M Lal, Efficien t Cancellable Biometric Key GenerationScheme for Cryptography. Int. J. Netw. Secur. **11**(2), 57–65 (2010)

[5]. AK Jain, K Nandakumar, A Nagar, in Security and privacy in biometrics. Fingerprint Template Protection: From Theory to Practice (Springer London, 2013), pp. 187–214

[6]. NK Ratha, S Chikkerur, JH Connell, RM Bolle, Generating Cancellable Fingerprint Templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)

[7]. A Ross, AK Jain, Information fusion in biometrics. Pattern Recognit. Lett.**24**, 2115–2125 (2003)

[8]. A Bodo, Method for Producing a Digital Signature with Aid of Biometric Feature. German Patent DE 4243908A1 (1994)

[9]. JH RM Bolle, S Connell, NK Pankanti, AW Ratha, Senior, Guide to Biometrics.(Springer-Verlag, New York, 2003)

[10]. NK Ratha, JH Connell, R Bolle, Enhancing Security and Privacy in Biometric-Based Authentication System. IBM Syst. J. **40**(3), 614–634(2001)

[11]. S Kanade, D Camara, E Krichen, D Petrovska-Delacr˜etaz, B Dorizzi, Evry F, in Proceedings of 6th Biometrics Symposium (BSYM 2008). Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris (Tampa, Florida, USA, 2008), pp. 59–64

[12]. S Kanade, D Petrovska-Delacr˜etaz, B Dorizzi, in Proceedings of FourthIEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington, DC, USA, 2010. Generating and sharing biometrics based session keys for secure cryptographic applications, (2010), pp. 1–7

[13]. A Jain, U Uludag, Hiding Fingerprint Minutiae in Images. in Proceedingsof Third Workshop on Automatic Identification Advanced Technologies (AutoID), (Tarrytown, New York. USA, 97–102 (2002)

[14]. A Jain, U Uludag, Hiding Biometric Data. IEEE Trans. Pattern Anal. Mach.Intell. **25**, 1494–1498 (2003)

[15]. N Agrawal, M Savvides, in Proceedings of IEEE Computer Society Conferenceon Computer Vision and Pattern Recognition. Biometric data hiding: A 3factor authentication approach to verify identity with a single image using steganography, encryption and matching (Miami Beach Florida, 2009), pp. 85–92

[16]. A Juels, M Wattenberg, in Proc. 6th ACM Conf. Computer and Communications Security, ed. by G Tsudik. A fuzzy commitment scheme (ACM New York, NY, USA, 1999), pp. 28–36

[17]. C Rathgeb, A Uhl.Context-based biometric key generation for Iris. IETComput. Vis. **5**(6), 389–397 (2011)

[18]. C Yao-Jen,WZhang, T Chen, in Proceedings of IEEE International Conference on Multimedia and Expo (ICME'04), Taipei, 2004, Vol. 3. Biometrics-based cryptographic key generation (IEEE, 2004), pp. 2203– 2206

[19]. N Lalithamani, KP Soman, in the 2nd International Conference on Computer Science and Information Technology. Towards Generating Irrevocable Key for Cryptography from Cancelable Fingerprints (Beijing China, 2009), pp. 563–568

[20]. N Lalithamani, KP Soman, Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme.Eur. J. Sci. Res. **31**(3), 372–387 (2009)

[21]. V Lokeswara Reddy, a Subramanyam, P Chenna Reddy, Implementation of LSB Steganography and its Evaluation for Various File Formats. Int. J.Adv. Netw. Appl. **02**(05), 868–872 (2011)

[22]. A Ross, K Nandakumar, AK Jain, Handbook of Multibiometrics. (Springer-Verlag, Berlin, Germany, 2006)

[23]. Fingerprint Verification Competition FVC2000, [Online]. Available: http://biascsr.unibo.it/fvc2000

[24]. Fingerprint Verification Competition FVC2002, [Online]. Available: http://biascsr.unibo.it/fvc2002

[25]. Fingerprint Verification Competition FVC2004, [Online].Available:http://biometrics.cse.msu.edu/fvc04db/index.html

[26]. R Cappelli, an Erol, D Maio, D Maltoni, in Proceedings of 15th International Conference on Pattern Recognition, 2000, vol. 3. Synthetic Fingerprint Image Generation, (2000), pp. 475–478

[27]. C Watson, M Garris, E Tabassi, C Wilson, M McCabe, S Janet, Ko K, User's Guide to NIST Biometric Image Software (NBIS). (National Institute ofStandards and Technology, Gaithersburg, MD, 2007)
[28]. Barman et al. EURASIP Journal on Information Security (2015) 2015:3 Page 17 of 17
[29]. A Rocha, W Scheirer, T Boult, S Golden stein, Vision of the unseen: Current trends and challenges in digital image and video forensics. ACM Comput.Surv. **43**(4), 26:1–26:42 (2011)
[30]. A Westfeld, A Pfitzmann, in Proc. Information Hiding, 3rd Int',l Workshop. Attacks on Steganographic Systems (Springer Verlag, 1999), pp. 61–76
[31]. S Dumitrescu, Wu Xiaolin, N Memon, in International Conference on Image Processing, (ICIP 2002), vol.3, no., 24-28. On steganalysis of random LSBembedding in continuous-tone images (Rochester, New York, USA, 2002), pp. 641–644
[32]. J Fridrich, M Goljan, Du Rui, Detecting LSB steganography in color, andGray-scale images. Multimedia IEEE. **8**(4), 22–28 (2001).