VOL. 10, NO. 6, APRIL 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

A SECURED BIOMETRIC FRAMEWORK FOR MULTIMEDIA CONTENT PROTECTION

M. Gobi[1] and D. Kannan[2]
[1]Chikkanna Government Arts College, India
[2]Nehru Arts and Science College, India
E-Mail: mgobimail@yahoo.com

ABSTRACT

The multimedia content protection has become a boon for an IT industry nowadays. This scheme is based on layered encryption/decryption involving biometric authentication. Utilization of fingerprints as keys in encryption/decryption procedures eliminates the feasibility of illegal key sharing, which hampers the content protection schemes based solely on traditional keys. The computation times required for the necessary encryption and decryption processes are provided for AES symmetric-key system and HECC asymmetric-key system. These times show the applicability of the method. Utilization of widely available encryption/decryption systems (e.g., AES and HECC) increases the applicability even further. Custom hardware chips will reduce these times in future applications.

Keywords: biometric framework, multimedia content protection, encryption, fingerprint verification.

1. INTRODUCTION

In the modern digital world, multimedia data (e.g., image, video, and audio) offers various opportunities to a pirate user, such as high-fidelity and rapid duplication: the generated copies are exactly the same as the original data, and copying is very fast. The uses of digital techniques are creation, editing and distribution of data. Contrariwise, analog techniques (e.g., printing and scanning an image) are relatively time consuming and they lead to quality degradation (e.g., due to printer noise). As a result of another advantage of digital techniques, the widespread usage of Internet provides additional channels for a pirate to quickly and easily distribute copyrighted digital content to a large number of users without the fear of being tracked.

Hence, multimedia data owners and their legal distributors are raising concerns about the loss of considerable amounts of revenues and its adverse effects on the creation of novel material and its timely distribution. As a result, the protection of multimedia content is now receiving a substantial amount of attention from the academia, multimedia industry, and regulatory government agencies.

Biometric technologies may add a new level of authentication and identification to applications, but are not, however, without their risks and challenges. There are important technological challenges such as accuracy, reliability, data security, user acceptance, cost, and interoperability, as well as challenges associated with ensuring effective privacy protections.

2. TECHNIQUES TO PROTECT MULTIMEDIA DATA

Two of the most commonly used methods for the protection of intellectual property rights (IPR) of multimedia data are digital watermarking and cryptography:

2.1 Digital watermarking

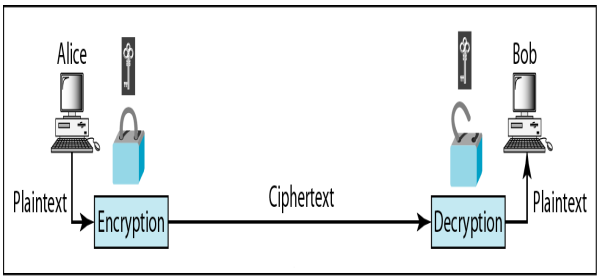
The embedding of information about the data into the multimedia data is called Digital watermarking. Currently, there is no watermarking technique that is robust to all possible attacks that can be mounted against it by the pirates (e.g., filtering, cropping, format change that results in the erasure of, duplication of, or ambiguity about embedded watermarks). As a result, this solution cannot eliminate the cited problems of piracy completely.

2.2 Cryptography

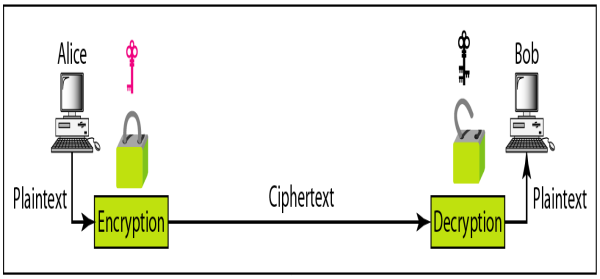
In traditional cryptographic systems, one or more keys are used to convert the plaintext (i.e. data to be encrypted: audio files) to cipher text (i.e. encrypted data: encrypted audio files). The encrypting key(s) maps the plain text to essentially a sequence of pseudo random bits (modern crypto algorithms are designed with this criteria), that can only be mapped back to the plain text using the appropriate decrypting key(s). Without the knowledge of the correct decrypting keys, the conversion of cipher text to the plain text is infeasible considering time and cost limitations. Hence, the cipher text is secured: even if an attacker obtains the cipher text, she cannot extract useful information (i.e. plain text) from it. Here, the plain text can be any data that needs to be stored or transmitted securely: financial transactions, e-mail communication, health records, fingerprint images, secret cryptographic keys, etc.

Figure-1 shows block diagrams of symmetric and asymmetric key cryptographic systems, in the realm of two entities that want to communicate securely (denoted as Alice and Bob). In the symmetric system, the decrypting key is the same as the encrypting key (namely, Alice and Bob share the key). Whereas in the asymmetric system, the decrypting key is not the same as the encrypting key, and it is only known to the recipient of the message: Alice can (DES), or asymmetric key system RSA, Elliptic Curve Cryptography (ECC) and Hyper Elliptic Curve Cryptography (HECC)) have high

theoretical and proven security. That is, there are no publicly known feasible procedures to invert the associated cipher text back to the plain text, given the computational resources (processor speed, processor quantity, and storage capacity) available to attackers today. As a result, encryption of multimedia data can be utilized to eliminate the problems of unauthorized copying and distribution: the data will be useless without the knowledge of the correct encrypting and decrypting keys. But this solution also has problems, as explained below.



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

Figure-1. Traditional cryptography: (a) symmetric key cryptography, (b) asymmetric key cryptography.

2.3 Limitations of Cryptography for multimedia data protection

Suppose Alice has an encrypted multimedia file, and assume that a pirate web site or a pirate user, Bob, is distributing this file. In order for Alice to use the file, she must also have the correct key(s) to decrypt the data. Alice can obtain the key(s) via legal means, e.g., receiving them after registering herself at the legitimate web site associated with the content. This way the content provider has the information about the user (Alice) who is about to view/play/listen to the protected content, and it has the means to charge Alice for this privilege. However, Alice can also obtain the key via pirated means (e.g., Bob sends Alice the correct key, in addition to the encrypted file), which eliminates the security provided by the encryption instantly. This illegal sharing of keys (i.e. key management problem) is a big drawback of any content protection scheme based on traditional cryptography.

2.4 To improve Cryptographic algorithms

An additional source of information that can be introduced to the encryption process is related to the attributes of the physical system (hardware or software) utilized by the consumers of multimedia data. For example, the hard disk (HD) serial number, the operating system number, computer IP address, etc. can be used as keys (or generators for keys) in the encryption process. In this scenario, the decoder checks these entities in a host computer and, if they are not the ones used during encryption, the data cannot be decoded correctly (hence, if Alice is not using a computer that has exactly the same credentials as those of Bob's, she will not be able to play the data). Here, it is assumed that the hardware identifiers cannot be tampered with, for example, not only can Bob not easily send his hard drive to Alice, but also Alice cannot tamper with her own hard drive serial number to imitate Bob's hardware credentials. But a legitimate user may want to play the multimedia file in multiple systems, such as a notebook, desktop computer, or PDA. Using hardware identifiers in the encryption/decryption processes eliminates such a possibility.

Another possible solution to illegal sharing of keys is to use biometric characteristics of the users. Assuming that the biometric system is secure Information about the feasibility of possible attacks can be found, introducing the biometric data of the user into the encryption/decryption processes (as keys or key generators) can increase the security of the digital content and decrease the feasibility of its illegal utilization. This would be equivalent to substituting the keys with biometric data (e.g., fingerprint features). For example, in the scenario mentioned earlier where Bob sent Alice a pirated file, now Alice would need to present Bob's finger to correctly decode the pirated data. The feasibility (with respect to time, cost, and required knowledge) of Alice replicating Bob's fingerprint features at her site is considerably less than obtaining traditional encryption keys from Bob. Hence, this solution has the potential to alleviate the piracy of copyrighted multimedia data, if yet another problem can be solved.

3. BIOMETRIC VARIABILITY AND CRYPTOGRAPHY

There is a big challenge to be overcome in using biometric signals as keys in encryption/decryption processes: biometric signals are *not* invariant over time. That is, even legitimate users of the system may not be able to decrypt the files that were encrypted with a previous acquisition of their biometric characteristics. For example, in the case of fingerprints, multiple impressions of a finger change because of improper placement of the finger on the sensor, sensor noise, dry or dirty fingers and cuts and bruises on them (Figure-2).

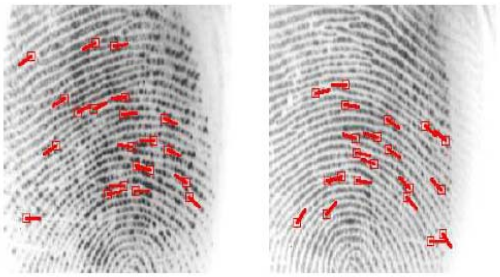


Figure-2. Intra-class variability of biometric signal: two different images of the same finger, with overlaid minutiae Intra-class variations in the biometric signals lead to non-invariance of features.

For example, Figure-2 shows the extracted minutiae features overlaid on the fingerprint images. As a result, biometric data cannot be used directly to define a key in a digital signature system. Note that, although these changes in biometric data are small, the cryptographic system becomes useless if the intra-class variability results in even a 1-bit change in the generated key. Traditional cryptographic systems work only if the key used during encryption is identical to the key used in decryption. Note that, in spite of these intra-class changes, the biometric matcher will normally generate a "higher" similarity score between two impressions of Bob's fingerprints, compared to the case when the input pair consists of one fingerprint from Bob and one from Alice.

4. ALGORITHMS FOR A HYPER-ELLIPTIC CURVE CRYPTOSYSTEM (HECC)

The basis for the Hyper-elliptic curve cryptosystem is the Discrete Logarithm Problem which is described as follows:

"Let F_q be a finite field with q elements. Given 2 divisors, D_1 and D_2 in the Jacobian, determine $m \in Z$, such that $D_2 = mD_1$."

The following section describes the proposed HECC algorithm which exploits ElGamal technique for key generation process, encryption and decryption process which is named as HEC-ElG Algorithm (HEC-ElGA).

Algorithm for Public Key and Private Key generation
Input: The public parameters are hyper elliptic curve C, prime p and divisor D
Output: The Public key P_A and Private key a_A

a) $a_A \in_R N$ [choose a prime (a_A) at random in N]
b) $P_A \leftarrow [a_A] D$

[The form of P_A is (u(x), v(x)) representation which is referred to as Mumford representation]
c) return P_A and a_A

For the random prime number generation in step1, one can apply the probabilistic test of Robbin-Miller (Stallings 2002) or the deterministic test of AKS (Jin 2005). However, various researches have proved that it takes exponential time to determine the given large number is prime or not using AKS algorithm.

Encryption/decryption algorithm

In this section, we present the methodology for encryption and decryption. The message 'm' that is to be sent will be encoded as a series of points represented as (u(x),v(x)). The encoded message is referred as E_m. For the encryption and decryption process using HECC, we have used ElGamal method to design HEC-ElG Algorithm (HEC-ElGA). Details on ElGamal method can be had from (Avanzi and Lange, 2006). The algorithm works as follows: To encrypt and send a message to B, A performs the following steps.

- $k \in_R N$ (choose k as a random positive prime number in N)
- $Q \leftarrow [k]D$ (D is the Divisor of the HEC & The form of Q is (u(x),v(x)))
- $P_k \leftarrow [k]P_B$ (P_B:(u(x),v(x)) is receiver's(B's) public key)
- $C_m \leftarrow \{ Q , E_m + P_k \}$ (C_m :(u(x),v(x)) is the Cipher Text to be sent)

To decrypt Cipher text message, the Decryption algorithm works as follows:

To decrypt the Cipher Text C_m, B extracts the first coordinate 'Q' from the cipher text then multiply with its Private Key (a_B) and subtract the result from the second coordinate. This can be written as follows,

$$E_m + kP_B - a_B(Q) = E_m + kP_B - a_B(kD) = E_m + kP_B - k(a_B D) = E_m + kP_B - kP_B = E_m$$

In the above process, 'A' has masked the message E_m by adding kP_B to it. The 'A' know the value of k, so even though P_B is a public key, nobody can remove the mask kP_B. For an attacker to remove message, the attacker would have to compute k from the given D and [k] D i.e. Q, which is assumed very hard.

5. PROPOSED SYSTEM

We propose a scheme of secured biometric framework based on biometric matching, with the aim of eliminating the feasibility of the illegal key sharing problem. Further, to achieve robustness against biometric variance, we use a novel biometric data transfer protocol, as explained below.

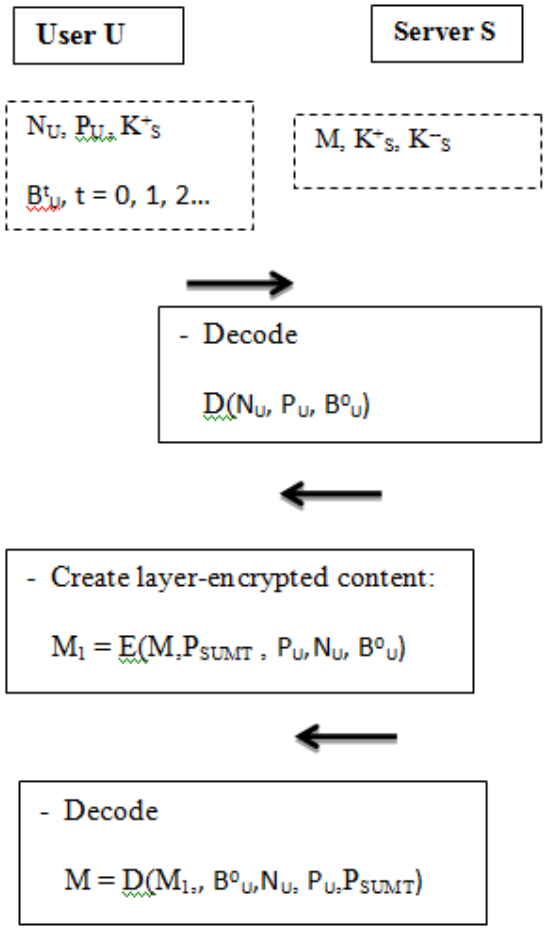


Figure-3. Data transfer structure.

Assume that there exist two communicating entities; the server *S* and the user *U*. The user *U* wants to receive the file M that resides at *S*. During data transfer, both asymmetric and symmetric key encryption schemes are used. In Figure-3, K^{+}_{S} and K^{-}_{S} denote the public and private keys of *S*, respectively. In the symmetric key system, *E*(*X; k*1*; k*2*; : : : ; kn*) denotes encrypting the file *X* first with key *k*1, then encrypting the resulting file with *k*2, and so on. Similarly, *D*(*Y; kn; kn*$_i$1*; : : : ; k*1) denotes decrypting the file *Y* , first with key *kn*, then decrypting the resulting file with key *kn*$_i$1, and so on. The Asymmetric cryptosystem based key generation for Server S that is useful for User to Server transaction.

The symmetric cryptosystem used to encrypt the message M. In this protocol we use AES for symmetric and HECC for Asymmetric cryptosystem. The data initially available at *S* and *U* are shown in respective columns inside dashed boxes in Figure-3. N_U is the name of the user *U*, P_U is the password of the user, and B^t_U (*t* = 0*;* 1*;* 2*; :*) denotes the biometric data (either as raw data, or feature vectors extracted from the fingerprint images as used in this study) of the user *U*, obtained at time *t*.

Now, we describe the biometric-based encryption and decryption processes in detail. First, Server key generation, K^{+}_{S} and K^{-}_{S} denote the public and private keys of Server *S* using *HECC*. The user encrypts N_U, P_U and B^0_U using the public key K^{+}_{S} of the server, and sends this encrypted data to the server. The server decodes these three pieces of information by using its private key K^{-}_{S}. Due to this asymmetric key scheme, only the server *S*, and not an intruder, can decode this information.

After checking the validity of the user credentials and related issues, the server creates a password P_{SUMT} (which is a function of the server *S*, user *U*, content M and a time stamp *T*, indicating the transaction date and time) using AES and sends it to the user after encrypting it with K^{-}_{S}. The user decodes this data by using the public key K^{+}_{S}.

The server creates the encrypted content M_1 by encrypting symmetrically, (using AES) Min a layered manner with the keys generated from P_{SUMT}, N_U, P_U and B^0_U. After appending the biometric data (B^0_U) to M_1 (necessary for eliminating the problem of biometric variance), another set of layered encryption is carried out as shown in Figure-3 to arrive at M_f. The server sends this file to the user. When the user wants to play the file, the keys used in encryption are used in reverse order to find M_2. Since this data (M_2) contains B^0_U, the biometric data obtained online from the sensor, B^1_U, can be matched with B^0_U. If there is a positive match, i.e., $B^0_U$and $B^1_U$are likely to be from the same finger, a final set of layered decryption is carried out to arrive at the actual multimedia content M. This will enable the media player to play the content M for user *U*. Note that if the user *U* wants to play the multimedia data at a different time, say, *t*2, then B^0_Uwill be matched with B^2_U and so on.

In this secured biometric framework scheme, we assume a "closed application", where the decrypted file is not stored at the user's computer but decrypted just before it is played. The biometric sensor, matcher, decryption module, media player and playing medium (e.g., monitor, speaker, etc.) are assumed to be connected together securely, where no tampering is possible.

When encryption and decryption are utilized in any system, the computational requirements become an important issue, since these additional operations (that increase the security) may render the overall system impractical. The computational requirements of an asymmetric key system are several orders of magnitude larger than that of a symmetric key system. Hence, we use the former just for processing relatively small amounts of data, such as user identity, password, etc., and the latter for encrypting the multimedia data itself (which can be huge in size; for example atypical 3 min. music encoded in MP3 format can occupy 5 MB).

In the next section, we provide the computing times measured for typical encryption and decryption processes via the Advanced Encryption Standard (AES), which is a successor for the traditional Data Encryption Standard (DES). AES provides stronger security, not only due to increased key size (128 bits for AES, and56 bits for DES) but also due to the design of the encryption algorithm itself. As a result, it is replacing DES and its

variants (e.g., 3-DES) in both government and commercial applications. We have also implemented the system using DES during the initial phases of this research.

As an alternative to generic systems such as AES and DES, cryptosystem architectures that are specifically designed for multimedia data can be used for reducing the time complexity and increasing the applicability of the system, especially for real-time applications.

6. EVALUATIONS OF FINGERPRINT VERIFICATION SYSTEM

The biometric matching in encryption leads to two additional considerations. Due to intra-class variations and inter-class similarities in biometric identifiers, every biometric system leads to some false rejects (conveyed via FRR or False Reject Rate) and some false accepts (conveyed via FAR or False Accept Rate). Below, we provide the results from recent government and academic evaluations of fingerprint verification systems:

6.1 FVC (Fingerprint Verification Competition) 2002

Publicly available (but small-sized) databases are used. The results can be good indicators for commercial system performances. The best system had an FRR of 0.28% at the FAR of 0.1%.FVC (Fingerprint Verification Competition) 2004: The best system had an FRR of 4.7% at the FAR of 0.1%. Note that the utilized databases were more complex (e.g., due to larger, exaggerated finger distortions) than those of FVC 2002, hence performance of state-of-the art in fingerprint matching may seem to be decreasing (cf. FRR's of 4.7% vs 0.28%). But this database difference is the key factor in the observed performance deviation.

6.2 NIST Fp VTE (Fingerprint Vendor Technology Evaluation) 2003

Government databases (large size) are used. The results can be good indicators for government application system performances. The best system had an FRR of0.4% at the FAR of 0.01%.

6.3 NIST SDK (Software Development Kit) Tests 2005

Again, large-sized government databases are used. The best system had an FRR of 0.99% at the FAR of 0.01%. The system evaluation architecture (vendor supplied hardware for Fp VTE vs. common government hardware for SDK Test) and utilized databases affect the performance deviation.

As an example, we will consider the FVC 2004 evaluation. For the cited FAR value of 0.1%, FRR of 4.7% would imply that a genuine user will not be accepted by the fingerprint matcher (approximately once in 20 tries) and therefore will not be able to play the multimedia content that she has legitimately acquired. While user habituation will decrease this error significantly, to eliminate this problem and reduce the FRR, the sensor may capture the same biometric more than once to increase the probability of a match.

Another issue in using biometric data is the time needed for verifying a user. The FVC 2004 study reported that the verification time for the best fingerprint matcher was 1.48 seconds (for a 1.41 GHz processor). This suggests that fingerprint matching is viable for use in encryption/decryption processes to secure multimedia data as outlined in Figure-3.

7. CONCLUSIONS

Here, we provide encryption and decryption times for the application of AES symmetric cipher on multimedia files. The standard key length in AES is 128-bits. Hence, the user ID (N_U), the user selected password (P_U), and server generated password (P_{SUMT}) are used directly as AES keys, where these values are 16-character strings composed of 8-bit ASCII code. The biometric data are generally larger in size; for example, a typical fingerprint image may generate a feature vector (composed of minutiae location and orientation data) that is more than 600-bits. Similarly, iris images generate a feature vector (IrisCode) with a 2048-bit length. These feature vectors can be converted to 128-bit keys via one-way hash functions, and then utilized as AES keys.

The basis for the Hyper-elliptic curve cryptosystem is the Discrete Logarithm Problem. The proposed HECC algorithm which used ElGamal technique for key generation process, encryption and decryption process. The server generates one time key for sending and receiving message. On a 3.2 Ghz Pentium 4 processor machine, the encryption (totally 7 epochs) and decryption (totally 7 epochs) of a 5 MB file took 1.8 seconds each. This time is acceptable since the decryption is only carried out once before playing the multimedia file. Furthermore, the utilization of special hardware chips can reduce these times substantially.

REFERENCES

C. V. Mosby, Bencheikh R. and L. Vasiu. 2005. Hybrid authentication systems. Proc. of the 2005 International Workshop in Wireless Security Technologies. pp. 130-137.

Bleha S. and M. S. Obaidat. 1993. Computer user verification using the perceptron. IEEE Transactions Systems, Man, and Cybernetics. 23(3): 900-902.

Bryan, W. L. and N. Harter 1973. Studies in the physiology and psychology of the telegraphic language. In The Psychology of Skill: Three Studies. E. H. Gardener and J. K. Gardner (eds.), NY Time Co. pp. 35–44.

Cavoukian A. 2005. Consumer Biometric Applications. Information and Privacy Commissioner of Ontario, Canada. http://www.ipc.on.ca/docs/cons-bio.pdf.

Clarke R. 2001. Biometrics and privacy. Notes available at:

http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html.

Daugman J. G. 1999. Recognizing persons by their iris patterns. In Biometrics: Personal Identification in Networked Society. A. Jain, R. Bolle, and S. Pankanti (Eds.), Kluwer. pp. 103-121.

Hill R. 1999. Retina identification. In Biometrics: Personal Identification in Networked Society. A. Jain, R. Bolle, and S. Pankanti (Eds.), Kluwer. pp. 123-141.

Jain A., L. Hong, S. Pankanti and R. Bolle. 1997. An identity-authentication system using fingerprints, Proc. of IEEE. 85(9): 1366.

Langeand L. and G. Leopold. 1997. Digital identification: it is now at our fingertips, Etimes. March 24, Vol. 946 (http://techweb.cmp.com/eet/823/).

Liu S. and M. Silverman. 2001. A practical guide to biometric security technology. IEEE Computer Magazine, January/February. pp. 27-32.

NIST. 2000. Report to the United States Congress, Summary of NIST Standards for Biometric Accuracy, Tamper Resistance and Interoperability.

Rhodes K. A. 2003. Information Security: Challenges in Using Biometrics. United States General Accounting Office. http://www.gao.gov/new.items/d031137t.pdf.