ISSN 2278-7763

Selectively Encrypted Pull-Up Based Watermarking of Biometric data

Prof. S. A. Shinde, Mr. Kushal S. Patel

[1] Assistant Professor, Vidya Pratishthan's College of Engg, Baramati, Maharashtra,India; [2] P.G. Student, Vidya Pratishthan's College of Engg Baramati, Maharashtra. Email: meetsan_shinde@yahoo.com, patelkushal4444@gmail.com.

ABSTRACT

Biometric authentication systems are becoming increasingly popular due to their potential usage in information security. However, digital biometric data (e.g. thumb impression) are themselves vulnerable to security attacks. There are various methods are available to secure biometric data. In biometric watermarking the data are embedded in an image container and are only retrieved if the secrete key is available. This container image is encrypted to have more security against the attack. As wireless devices are equipped with battery as their power supply, they have limited computational capabilities; therefore to reduce energy consumption we use the method of selective encryption of container image. The bit pull-up-based biometric watermarking scheme is based on amplitude modulation and bit priority which reduces the retrieval error rate to great extent. By using selective Encryption mechanism we expect more efficiency in time at the time of encryption as well as decryption. Significant reduction in error rate is expected to be achieved by the bit pull-up method.

Keywords : biometric watermark, amplitude modulation, bit pull-up method, bit priority, selective encryption, RNG mechanism.

1 INTRODUCTION

IN In user authentication system (human-by-machine authentication) the verification process of user identity takes place. is this person really who he/she claims to be? User authentication has become more complicated and difficult with the onset of the computer age. There are mainly three types of user authentication systems: knowledge-based authentication (what you know, e.g., passwords and PIN), Object-based authentication (what you have, e.g., physical keys), and ID based authentication (who you are, e.g., biometric ID such as voiceprint and signature, and physical ID such as passport and credit card) [1]. For authentication Passwords can be used as are excellent authenticators, but security is not provided once password is cracked. Passwords can be easily stolen by guessing or recording methods. Same is the case with other physical devices as well. Biometrics are useful to establish authenticity and for nonrepudiation of a transaction. There has been a significant surge in the use of biometrics for user authentication in recent years because of the threat of terrorism and the Web-enabled world [2].

In order to increase security, different types of authenticators should be combined. This also leads to increase in performance of system from external attacks [3]. The rapid growth of internet and related technologies has offered an unprecedented ability to access and redistribute digital contents. In such a context, data hiding is an important requirement which requires articulated solutions, encompassing technical, organizational and legal aspects. Though we are still far from such comprehensive solutions, in the last years watermarking techniques have emerged as an important building block which plays a crucial role in addressing the data hiding and ownership problem. Now days with emerging technology in computer science, an increased security of the biometric data is necessary in order to reduce attacks on system. Techniques based on steganography can be suitable for transferring critical biometric information from a client to a server and reduce the chances of illegal modification of the biometric data. Encryption can be applied to biometric models or templates after enrollment and will be decrypted during authentication. The encrypted templates are secured since they can be decrypted with a secret key. But, the problem is that encryption does not provide security once the data are decrypted. To overcome this problem, we use biometric watermarking method in which biometric data are still embedded into the host data which have been decrypted and will only be retrieved if a secret key for decryption is provided; therefore this provides security after decryption process as well. Biometric watermark is an invisible digital watermark that is embedded in a primary image and is imperceptible to the human eye but easily recoverable by a computer program. The locations where the data bits are embedded can only determined by using private key and this prevents possible cryptanalysis on the biometric data by great extent. The invisible watermark should not be easily removed by some multimedia signal processing techniques and should be retrieved from an altered image. The watermark should have following characteristics: unobtrusiveness, Robustness, Common geometric distortions (image and video data), Subterfuge attacks (collusion and forgery), Synchronization and Security. The invisible watermarking techniques need to be utilized in conjunction with encryption, site security and a proper legal framework [4].

Biometrics is usually classified as physical or behavioral types. The physical type includes biometrics based on

ISSN 2278-7763

stable body features, such as fingerprint, face, iris, and hand. The behavioral type includes learned movements such as handwritten signature, keyboard dynamics (typing), and gait. However, biometrics can be copied or counterfeited, so they cannot ensure authenticity or offer a guaranteed defense against repudiation.

There are various cryptographic techniques are available in the area of information security In symmetric key algorithm, both encryption & decryption uses the same key which is kept secrete from third party. [5-2]. Some sophisticated algorithms like DES, IDEA, RSA, AES etc. provides much security of confidential data and used for text & binary data. It is difficult to apply them directly on multimedia data as multimedia data are often of large size & require real time operation. As wireless devices are equipped with battery as their power supply, they have limited computational capabilities; therefore to reduce energy consumption we use the method of selective encryption of container image.

An efficient partial encryption algorithm is the potential solution to save power for wireless devices and at the same time to sufficiently protect the data. To achieve the encryption algorithm to cipher the selected part of the image container. This scheme use symmetric key algorithm with RNG mechanism.

2 BIOMETRIC WATERMARKING

In Biometric watermarking, image is viewed as combination of three channels (i.e. R,G,B). The blue channel is used to embed information. Blue channel is used because blue color has less sensitive to human eyes comparing with the red or the green ones, so better invisibility can be achieved. Extraction of bits will be handled by using the neighbor approximation technique in which average of all eight neighbors is considered. This method is used for invisible watermarking. In biometric watermarking, biometrics such as fingerprint, voice, and iris data will be converted to a bit sequence and then be embedded to a primary image. Consider the following example, where the bit sequence to be embedded is 0010 0001 and two watermarking techniques are used. After encoding and decoding by the first watermarking technique, the retrieved bit sequence is 0100 0001 with an error on the second and third bits. Using the second technique, the retrieved bit sequence is 0010 0010 with an error on the last two bits. If the number of wrong bits is regarded as error, we can see that the two watermarking techniques provide the same error (two wrong bits). However, if these embedded bit sequences are converted to unsigned 8-bit integers, and the difference between two integers is considered as an error, then the first watermarking method provides higher error than the second one does (the above sequences 0010 0001, 0100 0001, and 0010 0010 are corresponding to 33, 65, and 34, respectively.) From the above example, we can see that bits in different positions in a bit sequence will have different priorities for numerical information. The current amplitude modulation method for color images [4, 6] does not take into account this bit priority problem.

In Bit Pull-up based digital watermarking method based on amplitude modulation and priority, high priority bits should be embedded at good positions in the primary image. This achieves low error rate at extraction process. Experimental results show a significant error reduction for this bit pull-up-based method comparing with the other digital watermarking method based on amplitude modulation.

3 AMPLITUDE MODULATION AND BIT PULL-UP BASED DIGITAL WATERMARKING

Let $I(m, n)$ be a color image of size $m * n$. If the RGB color system is used, then

$$I(m, n) = \{R(m, n), G(m, n), B(m, n)\}.$$

Where

$$R_{(m,n)} \subseteq I$$
$$G_{(m,n)} \subseteq I$$
$$B_{(m,n)} \subseteq I$$

Let $S = (s1, s2, \ldots, sk)$ be the bit sequence of size k to be embedded in the image I. So after embedding data, set $I'(m, n) = \{R'(m, n), G'(m, n), B'(m, n)\}$. The amplitude modulation-based digital watermarking method embeds bits by modifying the blue channel in the color image I. In order to reduce error rate at retrieval end, each bit in S will be embedded d times at different positions in the image I. Therefore

$$I'(m, n) = \{R(m, n), G(m, n), B'(m, n)\}$$
[blue channel is changed]

Encoding Process: A pseudo-random position sequence $p = (p1, p2, \ldots, pd*k)$, where $p(t–1)*d+h = (i, j)$ representing row and column indices at which bit st is embedded the h-th time, is chosen to embed the bit sequence S. The sequence p is randomly generated by a pseudo-random generator based on a given secret key K, which is used as a seed to the generator. The sequence of pseudo-random positions can be calculated by Maclaurin *series* method. *Maclaurin series* is a representation of a function as an infinite sum of terms that are calculated from the values of the function's derivatives at a single point.

The error in this approximation is no more than $|x|^9/9!$. In particular, for $-1 < x < 1$, the error is less than 0.000003. This Maclaurin series is used here to reduce complexity of sequence generator. As Maclaurin series expansion is very much easy with parallel computing techniques, it is very much easy to compute sequence in average time complexity of $O(n/4)$. It can be seen that if the difference between $B''i,j$ and $B'i,j$ is low, then the retrieved bit is good. In this proposed method we are calculating Piwett operator to determining good positions in the container image.

Pewitt operator which calculates the gradient in a two dimensional image to determine good positions. The lower the

ISSN 2278-7763

gradient at a position is, the better this position is. Gradient ranges starting from 0 if the image contains no variations in pixels, if variations are less the Piwett value tends to zero and vice versa.

This Piwett function can be calculated by

$$Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Px_{di+2,dj+2} \right)$$

$$Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Py_{di+2,dj+2} \right)$$

$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2}$$

The position sequence *p* will be *rearranged* according to the increase of gradient. It is observed that the probability to retrieve embedded bit at position whose value of gradient factor is greater than 23 is less than 0.4924. Therefore we are discarding those positions from list. By discarding average quality and bad quality positions we get an array of positions which contains all good positions. We are now embedding data bit at this location. As the position is good bit is high prior. All the positions are good means all the bits are high priority bits. After this process the bits will be embedded sequentially.

The *t*-th bit in the bit sequence *S* will be embedded in the blue channel of the image *I* at *d* positions $p(t–1)*d+h$, …, $pt*d$ according to the following equation

$$B'i,j = Bi,j + stqLi,j$$

where *Li,j* is luminance at the position (*i*, *j*) and can be calculated as follows

$$Li,j = 0.299Ri,j + 0.587Gi,j + 0.144Bi,j$$

and *q* is a tradeoff between robustness and invisibility.

Decoding Process: Based on the secret key function *K*, the sequence $p(t–1)*d+h$, … , $pt*d$ is regenerated as shown in the encoding process. However, the gradient at each position needs to be calculated and depending on these gradient values, the sequence *p* will be rearranged.

$$Gx'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} Px_{di+2,dj+2} \right)$$

$$Gy'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} Py_{di+2,dj+2} \right)$$

$$G'_{i,j} = \sqrt{Gx'^2_{i,j} + Gy'^2_{i,j}}$$

As *R* = *R'*, we have *G' i,j* = *Gi,j* at all position (*i*, *j*) calculated. Therefore the sequence *p* after rearranging is the same in both the encoder and decoder processes.

If the original value *Bi,j* is given, we can determine the value of the embedded bit *st* by checking the difference δ between the retrieved value and the original value of the pixel being taken $\delta i,j = B'i,j - Bi,j$. The sign of the difference determines the value of the embedded bit. However, unfortunately, we do not have *Bi,j* at decoding process, so we try to estimate it, denoted as *B''i,j*, by using linear combination approximation of neighbor pixels. If the 8 neighbor pixels of the pixel (*i*, *j*) are considered, the value *B''i,j* is calculated as follows

$$B''_{i,j} = \frac{1}{8} \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B'_{i+di,j+dj} - B'_{i,j} \right)$$

and the approximated difference now is calculated as

$$\delta_{i,j} = B'_{i,j} - B''_{i,j}$$

The single bit *st* is embedded at *d* positions $p(t–1)*d+1$, …, $pt*d$, therefore we use the arithmetic average method to calculate the value δt

$$\bar{\delta}_t = \frac{1}{d} \sum_{t=1}^{d} (B'_{p(t-1)d+i} - B''_{p(t-1)*d+i})$$

The sign of δt is the estimated bit *s't* of the embedded bit *st*. The larger the absolute value of $\bar{\delta}_t$ is, the higher confidence of the estimation i.

$$s'_t = sign(\bar{\delta}_t)$$

Algorithm (Embedding data) :

Data elements : Sequence[ ], I : Image, I' : image, Piwett[ ] , n : no of bits in input data. s[ ] : bit stream, L[ ] : Luminance factor, x,n,l,d : iterators.

Step 1: Convert image input to bit sequence
Create bit_seq(image).
Step 2 : Generate sequence by secrete key function.
*for(x ← 1;x<12*d;x+=12)*
for(n ← 1;n<4;n++) // Error factor is 4,
*sign ← -1*sign;*
denom ← 1;

ISSN 2278-7763

```
for ( i= 1; i<=((2*n)+1); i++)
        denom ← denom* i;
    for ( i ← 1; i<=((2*n)+1); i++)
        multiplier ← multiplier *x;
        seq[pos]←sign*(multiplier/denom);
                seq[pos]←seq[pos]mod
                                size_of_biometric_data;
        pos ←pos+1;
    end for;
end for;
```

Step 3 : Operate Pixwett function

$$Gx_{i,j} = \left(\sum_{} \sum_{} B_{i+di,\, i+di} Px_{di+2,di+2} \right)$$

$$Gy_{i,j} = \qquad Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,\, j+dj} Px_{di+2,dj+2} \right)$$

$$G \qquad Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,\, j+dj} Py_{di+2,dj+2} \right)$$

$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2}$$

```
    end for
Step 4:  Discarding bad positions
        for i=seq[0] to seq[d*n] do
            if ( pewitt[i]< Max_Threshold ) then
                discard seq[i] from list;
Step 5: Sort seq[ ] by gradient values
                sort( seq[ ],pewitt[ ]);
    Step 6:  Embed bits at Good positions
            for t=1 to n do
        for i=1 to d do
                    p=(t–1)*d+i ;
                    B'=B[ seq[p] ]+ St q L[p];
                    I' [B[ seq [p] ] ] = B' ;
                end for;
            end for;
  Step 5:   End;
```

Algorithm for data extraction is same as embedding process, only we are c

Step 6: Extrac

for

$$\bar{\delta}_t = \frac{1}{d} \sum_{t=1}^{d} (B'_{p(t-1)d+i} - B''_{p(t-1)*d+i})$$

$$\bar{\delta}_t = \frac{1}{d} \sum_{t=1}^{d} (B'_{p(t-1)d+i} - B''_{p(t-1)*d+i})$$

```
        end for;
```

3 SELECTIVE ENCRYPTION ALGORITHM

In selective encryption is just to encrypt a certain portion of messages with less consumption of energy and time but at the same time data should be encrypted in order to secure data sufficiently [5]. In this algorithm need not required to encrypt all data contents; only the segments of data are encrypted. The data should be segmented in a standard pattern which involves sufficient uncertainty. The more confusion is involved, the security will be more and more effective is the cryptosystem. In Multimedia systems, tremendous audio and video data need to be transferred securely .Real time transmission has very much importance in the field of multimedia transmission. To encrypt whole multimedia data large time and computational power is required. This may affect on the timely transmission of data. In such circumstances, the design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant.

This algorithm aims to involve sufficient confusion into the encryption process, while providing satisfactory security of the message. In order to select the message randomly it uses the concept of Random Number Generation [8]

This partial encryption algorithm which uses the advantages of randomization method aiming to obtain sufficient uncertainties in the selection of the bit positions of a multimedia message. At the time of sending the message, message is converted into binary format and then random positions are determined. The data at the position of random positions will be encrypted. After that this encrypted segments are send through the communication channel by concatenating them with remaining bits of data at appropriate positions.

Algorithm (Encryption):

Data elements : Length : length of image, Sequence[ ], I : Image, I' : image , Ki :Symmetric key, n : no of bits in input data. s[ ] : bit stream, SendData[] , x,n,I,d : iterators.

```
Step1: Length= No_of_bytes(Image);

Step 2: no_of_positions = (70 * Length/100)+C;
            // The generated bit positions should be higher
              than the 70% of the determined Length.
          Sequence = Genete_random();

Step 3: for i=1to Length do
            If(i= Sequence[i])
              Inparam=I[Sequence[i]];
              SendData= SendData+ Encrypt(Inparam ,Ki);
            Else
              SendData= SendData+ I[Sequence[i]];
              end for;
Step 4 : I'= SetImage(SendData[]);

Step 5 : end;
```

Algorithm Decryption:

Data elements : Length : length of image, Sequence[ ], I : Image, I' : image , Ki :Symmetric key, n : no of bits in input data. s[ ] : bit

ISSN 2278-7763

stream, RecvData[] , x,n,I,d : iterators.

Step1: Length= No_of_bytes(Image);

*Step 2: no_of_positions = (70 * Length/100)+C;*
// The generated bit positions should be higher than the 70% of the determined Length.
Sequence = Genete_random();

Step 3: for i=1to Length do
If(i= Sequence[i])
Inparam=I'[Sequence[i]];
RecvData= RecvData+ Decrypt(Inparam ,Ki);
Else
RecvData= RecvData+ I[Sequence[i]];

end for;
Step 4 : I'= SetImage(RecvData[]);

Step 5 : end;

4 CONCLUSION

We have proposed a new biometric watermarking method based on amplitude modulation and bit priority level using Pull-Up method. While inheriting security characteristics such as anti-attack from the original method, the proposed method is very useful in biometrics applications, where numeric feature or model values of fingerprint, voice, or iris need to be embedded to an image. The Security is based on two keys which are very hard as such to break. Invisible Partial encryption provides more security with less computational complexity and power consumption. The proposed method has been evaluated and compared with the current digital watermarking method based on amplitude modulation. Since the errors are nearly zero in the proposed method, no changes have been affected to biometric authentication systems.

5 REFERENCES

[1] Tuan Hoang, Dat Tran, Dharmendra Sharma "Bit Priority-Based Biometric Watermarking", University of Canberra, Proceedings of the IEEE, pp. 191-195, 2008.

[2] L. O'Gorman. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, 2003

[3] R.M. Bolle, J. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. Biometrics 101. IBM Research Report, IBM T. J. Hawthorne, New York, 2002

[4] F. Bao, R. H. Deng,"Light-Weight Encryption Schemes for Multimedia Data and High-Speed Networks", Proceedings of IEEE Global Telecommunications Conference, pp. 271–350, 2007.

[5] Yonglin Ren, A. Boukerche, L. okdad,"Performance Analysis of a Selective Encryption Algorithm for WirelessAd-Hoc Networks", Proceedings of IEEE Wireless communications and networking conference, pp. 1038- 1043,2011.

[6] M. Aikawa, K. Takaragi, Eds.,"A Lightweight Encryption Method Suitable for Copyright Protection", IEEE Transactions on Consumer Electronics, Vol. 44, pp. 902–910, 1998.

[7] M. Kutter, F. Jordan, and F. Bossen, "Digital Watermarking of Color Images Using Amplitude Modulation", Journal of Electronic Imaging, vol. 7, no. 2, pp. 326 – 332, 1998 194

[8] N. M. Thamrin, G. Witjaksono, A. Nuruddin, Eds.,"An Enhanced Hardware-based Hybrid Random Number Generator for Cryptosystem", Proceedings of International Conference on Information Management and Engineering, pp. 152–156, 2009.

[9] S.P. Mohanty, K.R. Ramakrishnan, M.S. Kankanhalli, "A DCT domain visible watermarking technique for images", in Proceedings of Multimedia and Expo IEEE International Conference, vol. 2, pp. 1029 – 1032, 2000

[10] I.J. Cox et al., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, vol. 6, no. 12, pp. 1673 – 1687, 1997

[11] R. G. Wolfgang, and E. J. Delp, "A Watermark for Digital Images", Proc. IEEE Intl. Conf. on Image Processing, ICIP-96, vol. 3, pp. 219 – 222, 1996

[12] W. Zhu et al., "Multiresolution Watermarking for Images and Video: A Unified Approach", Proc. IEEE International Conf. on Image Processing, vol. 1, pp. 465 – 468, 1998

[13] P. Loo, N. Kingsbury, "Watermark detection based on the properties of error control codes", IEE Proceedings Vision, Image and Signal Processing, vol. 150, no. 2, pp. 115 – 121, 2003

