International Journal of Computational Intelligence Systems, Vol. 4, No. 4 (June, 2011), 596-605

Content-based Image Hiding Method for Secure Network Biometric Verification

Xiangjiu Che[1,*], Jun Kong[2], Jiangyan Dai[2], Zhanheng Gao[1], Miao Qi[2,*]

[1] *College of Computer Science and Technology, Jilin University, Changchun, 130012, China*
[2] *School of Computer Science and Information Technology, Northeast Normal University, Changchun, 130117, China*

Abstract

For secure biometric verification, most existing methods embed biometric information directly into the cover image, but content correlation analysis between the biometric image and the cover image is often ignored. In this paper, we propose a novel biometric image hiding approach based on the content correlation analysis to protect the network-based transmitted image. By using principal component analysis (PCA), the content correlation between the biometric image and the cover image is firstly analyzed. Then based on particle swarm optimization (PSO) algorithm, some regions of the cover image are selected to represent the biometric image, in which the cover image can carry partial content of the biometric image. As a result of the correlation analysis, the unrepresented part of the biometric image is embedded into the cover image by using the discrete wavelet transform (DWT). Combined with human visual system (HVS) model, this approach makes the hiding result perceptually invisible. The extensive experimental results demonstrate that the proposed hiding approach is robust against some common frequency and geometric attacks; it also provides an effective protection for the secure biometric verification.

Keywords: Content Correlation, Principal Component Analysis, Particle Swarm Optimization, Discrete Wavelet Transform, Network-based Biometric Verification

1. Introduction

Recently, biometrics-based techniques using distinct physiological or behavioral characteristics are becoming increasingly popular. The biometric verification systems have many advantages over the traditional knowledge-based verification systems, but their vulnerability to attacks result in decreasing security. For instance, when biometric data transmits over the network for remote verification, it might subject to unintentional or intentional attacks, which will tamper the content of biometric data and degrade the performance of biometric systems. Schneier[1] pointed out that the verification system worked well when the system could guarantee the legitimacy of the biometric data. Moreover, while biometric data provides uniqueness and stability for accurate identity verification, they could not provide the secrecy[2]. Consequently, protecting the security and integrity of biometric data becomes a critical problem for ensuring valid biometric verification.

Cryptography, watermarking and steganography technologies are effective tools for communicating secret messages and data protection[3-5]. Researchers have proposed various methods to protect biometric data through information hiding techniques[6-15]. According to the hiding domain, there are spatial domain methods[8], frequency domain methods[6,11,12], and combination method of spatial and frequency domain[15]. The validity and feasibility of these methods have been indicated by experimental results. However, most of these ideas originated from digital watermarking and embedded watermark into another biometric image, or hidden one or more biometric features into another biometric image directly for secure verification[9-11,14]. In particular, the cover image is a biometrics, whereas the watermark can either be a biometrics, or other biometric features. Due to the specific characteristics of the biometric image, it is prone to be intercepted or destroyed by attackers resulting in degrading the security of transmission. For security purpose, M.K. Khan et al embedded secret data into an inconspicuous cover file to conceal the secret communications[13]. In their work, the iris template was encrypted firstly by using the biometric key and then hidden into another unrelated cover image using DWT method. However, the hiding capacity was not high. In addition, most existing literatures paid more attention to the robustness evaluation, but ignored the quality evaluation of the watermarked images/stego-images.

For most existing image hiding methods, the secret image was only embedded through modifying the

* Corresponding authors
E-mails: chexj@jlu.edu.cn, qim801@nenu.edu.cn

content of the cover image [10,16,17]. As we analyze above, the cover image holds some content related to the secret image. It is preferred that we could explore the content of the cover image related to the secret image through some statistical methods. Namely, the cover image not only plays the role of hiding carrier, but also carries a part of content related to the secret image. Based on the correlation analysis and spatial domain, a multimodal hiding approach was presented to protect the security and integrity of transmitted biometric images, and the experimental results and analysis indicated that it provided good hiding performances[18]. Although the method could resist some frequency and geometric attacks, it was fragile to compression attack. In addition, for a biometric image, four related sub-blocks were located in the cover image resulting in high computational complexity and weak real-time. Moreover, even though it could provide high security, the secret key was also complex.

In order to improve the hiding performances, this paper proposes a frequency hiding approach for secure biometric verification. The proposed approach embeds the secret image into a public cover image to avoid the attacker's attention. In particular, the correlation between the cover image and the biometric image is implemented using PCA and PSO algorithms. In order to analyze the correlation thoroughly, inconsecutive regions are located to represent the biometric image as much as possible. As a result of the correlation analysis, the related part of biometric image can be represented by located regions through projection and reconstruction. Finally, combined with HVS, the unrepresented part is hidden into the cover image using DWT to obtain the stego-image for transmission. At the receiver end, the biometric image is extracted through executing the reverse process of representation and embedding for verification. The extensive experimental results show that the proposed method not only guarantees the imperceptibility, but also resists some common attacks. The proposed content-based correlation analysis approach exhibits the following advantages: (1) high security, the biometric image is hidden into another public cover image for transmission to degrade the destructive possibility that hackers or attackers are sensitive to biometric images; (2) perfect stego-image quality, the peak signal-to-noise ratio (PSNR) of stego-image is higher than 44dB; (3) large hiding capacity, the average capacity is 0.1094 bit/pixel; (4) good robustness, the proposed approach is robust against some common attacks, such as compression, filtering, scaling and cropping.

The remainder of this paper is organized as follows. The proposed biometric image hiding method is presented in Section 2, including the descriptions of correlation analysis, information embedding and extraction. Section 3 gives the experimental results and discussions, followed by the conclusions and future work in Section 4.

2. The Content-based Hiding Approach

In this paper, the palmprint is the biometric image for secret transmission. The aim of hiding is to protect its integrity and security for effective network-based verification. The flowchart of proposed hiding approach is shown as Fig.1.

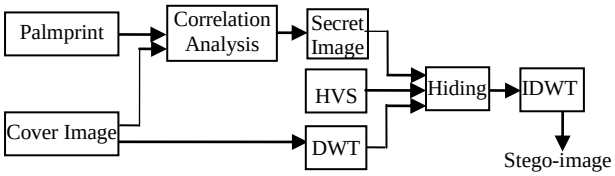


Fig. 1. The flowchart of proposed hiding approach.

2.1. *Correlation analysis*

The aim of correlation analysis is to represent the biometric image adequately by using the abundant information of the cover image. Given a transmitted palmprint I ($m\times n$), a region Y ($m\times n$) in the cover image will be located to represent I. Here Y is not a continuous region necessarily. Each row of Y is regarded as one sample; the first orthonormal eigenvector V_1 can be computed by PCA method[19], which can reduce data dimensionality by performing a covariance analysis among variables. Then, we project I onto V_1 to get the first projected principal component F_I. Thus, I can be represented (or reconstructed) by the first orthonormal eigenvector V_1 of Y and the projected principal component F_I as:

$$\tilde{I} = F_I V_1^T \tag{1}$$

The difference between I and $\tilde{I}$ is the unrepresented part with the content of Y, and different Y will lead to different represented result. We hope the region Y can

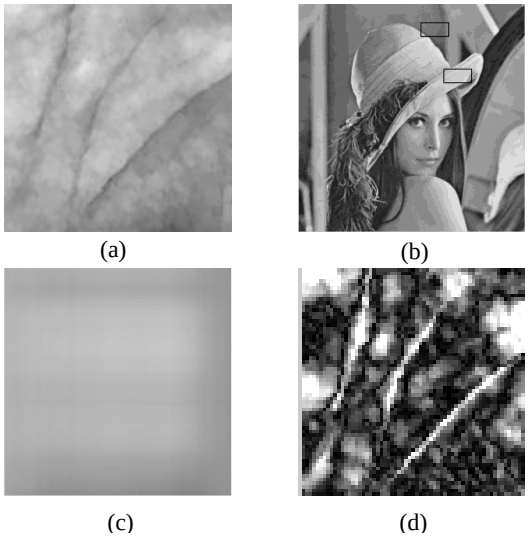
represent I as much as possible. That is, smaller difference is desired. Consequently, the selection of region Y can be regard as an optimization problem. In this paper, PSO algorithm is employed to locate the region Y. PSO is a population-based heuristic search method, which is inspired by social behavior of bird flocking or fish schooling[20]. In the past several years, PSO was used to solve optimization problems in some fields successfully[21,22,23]. In this paper, the fitness function of PSO can be defined as:

$$\text{Min } Fun = \sum_{i=1}^{m}\sum_{j=1}^{n}\left|I(i,j) - \tilde{I}(i,j)\right|. \quad (2)$$

The positions of Y and reconstruction coefficients F_I are stored as secret key. As the randomness of PSO and random selection of the cover image, the secret key holds high randomness and security. Therefore, it is unpredictable and difficult to be deciphered by attackers. Once the region Y is located, the residual image E can be obtained by:

$$E = I - \tilde{I}. \quad (3)$$

Figure 2 shows the result of correlation analysis. In Fig. 2(b), two black rectangle regions are sub-regions to form the reconstructed regions Y. Since E is the result of subtraction, the negative pixel values may be generated. The histograms of Fig. 2(a), Fig. 2(c) and Fig. 2(d) are shown in Fig. 3, respectively.



(a) (b) (c) (d)

Fig. 2. (a) Palmprint, (b) cover image, (c) reconstructed palmprint, (d) secret image (shown as absolute difference between (a) and (c) and magnified by a factor 8).

Fig. 3 shows that the reconstructed palmprint holds most energy of the original palmprint. Moreover, the absolute values of all pixels in the secret image are less than 60, which mean that the residual image has much less energy than the original palmprint. Furthermore, it can be represented with fewer bits.

2.2. *Secret image hiding*

After the residual image is obtained, it will be embedded into the cover image as secret image. Currently, information hiding techniques can be broadly classified into two categories: spatial domain and transform domain. Generally, the former provides large hiding capacity but less complexity, and the latter is resistant against attacks. In order to guarantee the integrity of biometric for effective verification, the robustness is more desirable. Therefore, transform domain methods are perfect candidates. Among the transform domain techniques, the biometric data hiding techniques based on DWT are more popular. As DWT can provide both frequency and spatial domain characteristics which are compatible with the HVS, we adopt HVS model to select the significant DWT coefficients for embedding the secret data[24].

2.2.1. *Secret image conversion*

In order to embed conveniently, the secret image is represented by a binary sequence. The process in detail is as follows:

Step 1: Divide the secret image into two parts: sign part and digital part. The sign part is represented by a binary bit plane. For positive, the relative value of bit is assigned to zero, otherwise, one is assigned.

Step 2: Represent the digital part using a binary stream. Statistical results show that most values belong to the interval [-64, 64]. So, each pixel can be represented by six bits. Only very few values might take up seven bits. For the consistency of representation, only the last six bits are preserved even if some values take up seven bits. Thus, each pixel of the secret image is represented by seven bits, the first bit is sign and the other six bits are digital. To clarify, four examples of representation are shown as:

$$8 \mapsto \underline{0}\ \underline{001000} \quad -13 \mapsto \underline{1}\ \underline{001101}$$
$$44 \mapsto \underline{0}\ \underline{101100} \quad -25 \mapsto \underline{1}\ \underline{011001}$$

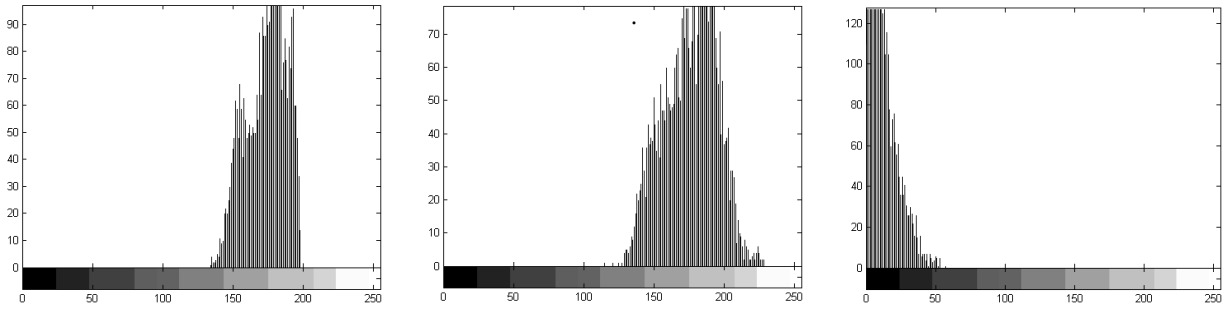


Fig. 3. The histograms of Fig. 2(a), Fig. 2(c) and Fig. 2(d).

Step 3: Connect the seven bits of each pixel orderly. Thus, the secret image with the size of $m \times n$ can be converted into a binary sequence $B = (B_k \in \{0,1\}, k = m \times n \times 7)$.

2.2.2. *Secret image embedding and extraction*

Generally, the low-frequency sub-band of DWT concentrates most of its energy, and common image processing and attack operations have weak influence to it. Thus, the low-frequency sub-band has good stability. Furthermore, in the case of adopting the same hiding algorithm and hiding capacity, embedding in the low-frequency sub-band has greater robustness and imperceptibility than in the detail sub-bands[25,26]. Therefore, the binary sequence of secret image is embedded into the low-frequency sub-band in our work.

To enhance the perceptual imperceptibility, the embedding regions are selected by using the HVS model[24]. In this model, texture and luminance are considered to reduce image distortion in the stego-image. The maximum number of data-embeddable bits at each pixel is recorded as an index image. Fig. 4(b) shows the index image of 'Lena' cover image, whose index values belongs to interval [0, 4].

(a) (b)

Fig. 4. (a) Cover image and (b) its index image.

Then, based on the ideas of literatures[24,26], the detailed processes of embedding and extraction are described as:

Embedding process

Input: Cover image ($M \times M$) and binary sequence $B = (B_k \in \{0,1\}, k = m \times n \times 7)$

1. Transform the cover image into wavelet coefficients by using one-level wavelet transform, and obtain the low-frequency coefficients *V*.
2. Compute the index image of *V* using HVS model. The coefficients, which have the larger value (sorting in descending order) in the index image are considered as significant coefficients and used for embedding the binary sequence.
3. Add bit sequence to significant coefficients using:

$$V_{ij} = V_{ij} + \alpha \times B(k),\ i, j = 1,\ 2, \cdots,\ M/2,$$

where α is the embedding strength.

4. Apply the inverse DWT to obtain the stego-image.

Output: Stego-image.

Extraction process

Input: Stego-image

1. Transform the stego-image and cover image into wavelet coefficients by using one-level wavelet transform, and obtain the corresponding low-frequency coefficients $V^{'}$ and *V*.
2. Compute the index image of *V* using HVS model. Extract the binary sequence from $V^{'}$ according to the index image of *V* with lager values by:

$$B_k^{'} = (V_{i,j}^{'} - V_{i,j}) / \alpha,\ i, j = 1, 2, \cdots, M/2, \text{ and } k = m \times n \times 7$$

3. If $B_k^{'} > T$, then $B_k^{'} = 1$; else $B_k^{'} = 0$,

where *T* is the decision threshold.

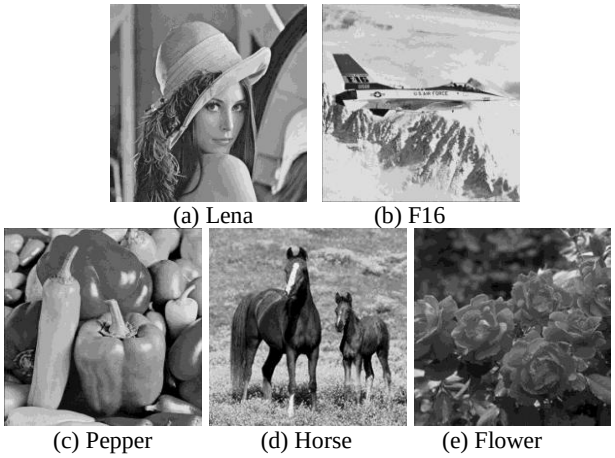
Output: Binary sequence.

At the receiver end, the binary sequence is first extracted from the stego-image. Each seven-bit is a group, the first bit is recorded as sign bit, and the remaining six bits are converted to decimal form as digital part. Then the secret image *E* is obtained by combing the sign part and digital part. Suppose that a part of extracted binary sequence is 01001001010010100010, the corresponding pixel values are 36 (0 100100), -18 (1 010010) and -6 (1 000110), respectively.

The reconstructed image can be obtained by using the secret key. First, the feature space V_1 of related regions in cover image can be computed by using PCA method. Then, the reconstruction coefficients F_I and feature space *V* are used to reconstruct the related part of palmprint $\tilde{I} = F_I V_1^T$. Finally, the secret image and reconstructed image are added to form the palmprint image for further verification.

3. Experiments and Discussions

The proposed hiding approach embeds the biometric image into the cover image for network-based biometric verification. Without lost of generality, five grayscale images (512×512) shown in Fig. 5 are used as cover image. Three of them come from the common images used widely in information hiding field[27,28] and the others from image retrieval database COREL (http://www.corel.com).



(a) Lena (b) F16

(c) Pepper (d) Horse (e) Flower

Fig. 5. The five cover images.

The biometric verification is performed on the palmprint database from Hong Kong Polytechnic University. In this paper, 1000 palmprints from 100 individuals are used to evaluate the performances of the proposed approach. Each individual provides ten images, and five images are used for training and the others for transmission test. The size of the original palmprint is 384×284 pixels, in the preprocessing stage, a region of interest (ROI) with size 64×64 is cropped for verification. In view of its advantages and effectiveness[29], two-dimensional principal component analysis (2DPCA) is used for feature extraction[30]. The similarity between two feature vectors is measured by Manhattan distance, and the nearest neighbor classifier is adopted for classification because of its simplicity and feasibility. For the verification results, the verification accuracy can reach the top point of 97.30% when the dimension in 2DPCA reduces to 8.

Two series of comparison experiments are performed to demonstrate the effectiveness and superiority of our method in the following. One experiment uses our proposed content-based correlation hiding approach (called EXP1); the other hides the original palmprint into the cover image directly without correlation analysis (called EXP2). That is to say, no correlation analysis procedure is taken into account in EXP2. Each pixel value of the biometric image is represented by eight binary bits to form the binary sequence, and the hiding capacity is

$$64 \times 64 \times 8 / (512 \times 512) = 0.1250 \text{ bit/pixel.}$$

The hiding process is the same as EXP1. In order to achieve a good compromise value among integrity, imperceptibility and robustness, we set T=0.5 and $\alpha = 8$.

At the stage of correlation analysis in EXP1, the number of sub-regions representing palmprint is firstly studied since the ability of reconstruction is affected directly by the located regions. In Table 1, four cases of sub-regions with two indicators are investigated. One indicator is the reduced multiples of energy (RME, defined as Eq. (4)) of the secret image compared with the original image; the other is the complexity of secret key, which is evaluated by the number of positions (N-p).

$$\text{RME} = \sum_{i=1}^{m}\sum_{j=1}^{n} I(i,j) / \sum_{i=1}^{m}\sum_{j=1}^{n} |E(i,j)|. \quad (4)$$

Since the aim of correlation analysis is to obtain the residual image with much less energy, larger RME value is desired. The larger RME illustrates that the cover image represents the palmprint better, and absolute values of each pixel in the secret image are smaller. It also means that the cover image can carry much information of the palmprint.

Table 1 shows that the related region *Y* formed by

multiple sub-regions can represent the palmprint image better than one successive region in view of RME. Undoubtedly, more positions N_p are stored for recovering the secret image for multiple sub-regions. In other words, the secret key is more complex. Moreover, the RME increases very slowly when N_r is larger than 2. Based on the comprehensive consideration of two indicators, two sub-regions are used for representation.

Table 1. The reconstructed results with different sub-regions.

Number of sub-regions	*1*	*2*	*3*	*4*
RME	14.81	15.90	16.06	16.21
N_p	2	4	6	8

Since each pixel of secret image is represented by seven bits in EXP1, the hiding capacity is

$$64\times64\times7/(512\times512)=0.1094 \text{ bit/pixel.}$$

Given a transmitted palmprint, the running time and computational complexity of each step are listed in Table 2.

Table 2. The running time of each step.

	Correlation Analysis	*Embedding*	*Extraction*	*Verification*
Time(*s*)	2.8	0.74	7.37	0.016
Complexity	$O(Tnd)$	$O(MN)$	$O(MN)$	$O(pD)$

In Table 2, *n* and *d* are the number and dimension of particle respectively, *T* is the time of iteration. *M* and *N* are the size of the cover image; *p* and *D* are the numbers of training sample and feature dimension respectively.

The total running time of our approach is about 11*s*, which proves it holds better real-time.

3.1. *Imperceptibility evaluation*

The imperceptibility is evaluated by peak signal-to-noise ratio (PSNR). Since each of the five cover images can be selected randomly as a carrier for a transmitted palmprint, the average PSNR value is computed for each type of stego-image. Fig. 6 shows the comparison results. In general, the image quality is acceptable if the PSNR value is greater than 35dB, and all PSNR values for both approaches are larger than 35dB. This indicates that both approaches can achieve the satisfactory imperceptibility. Furthermore, EXP1 has higher PSNR values than EXP2, and all PSNR values are larger than 44dB except the stego-image "Flower" of 43.90dB. The average value of these five types of stego-image is 44.03dB in EXP1 and 41.72dB in EXP2, which means that EXP1 provides better quality of the stego-images than EXP2 by 2.31 dB.

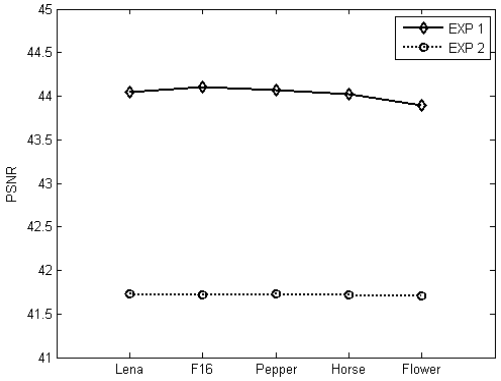


Fig. 6. PSNR values of EXP1 and EXP2.

The good imperceptibility of the proposed method is attributed to the content-based correlation analysis. As a result of correlation analysis in EXP 1, the total energy of the original palmprint is 15 times more than the secret image on average. Namely, the absolute value of each pixel in the secret image is very small. There are many zero elements when the secret image is represented using a binary sequence. In the embedding process, only small number of changed coefficients can guarantee the better stego-image quality. As seen from Fig. 3, most pixel intensities in the palmprint are between 120 and 200. Thus, most bits are one in the binary sequence of EXP2, which results in changing many coefficients for embedding. Moreover, since each pixel in EXP1 is represented by seven bits, the hiding capacity of EXP1 is less than EXP2 by 1/8. Through the above analysis, EXP2 is inferior to EXP1 from the perspective of imperceptibility; even tough it can gain good stego-image quality as well.

3.2. *Robustness evaluation*

For biometric image hiding applications, higher biometric accuracy and better robustness to attacks are desired. Higher or lower values of hiding metrics do not ensure higher performance of the biometric system. The objective of a biometric image hiding approach is to

provide additional security to the biometric system, but it is not easy to guarantee the integrity of biometric data under some malicious attacks. The usability of attacked biometric image for verification depends on the verification accuracy. In other words, the light quality degradation of biometric data can still ensure the validity of verification results.

Next, we test the variety of palmprint verification accuracy when the stego-images are subjected to some frequency and geometric attacks, such as JPEG compression, Gaussian filtering with 3×3 kernel, Gaussian noise, impulse noise, scaling and cropping. Most existing approaches performed each type of attack with one fixed factor. And some of them did not give the detailed attack parameter values, such as the mean and variance of Gaussian Noise and the standard deviation of Gaussian filtering.

In order to test the effect on the verification accuracy, different attack factors for each type of attacks are implemented. All these six types of attacks can be controlled easily by setting parameters except the cropping attack, e.g., and the compression ratio can control the compression quality of the stego-image. For the cropping attack, there are many cropping types. In this paper, area, shape and position, the three cropping factors are considered in the cropping types[31,32]. For example, cropped 'Lena' images are shown in Fig. 7, the numbers in brackets are the percentage of corresponding cropping areas.

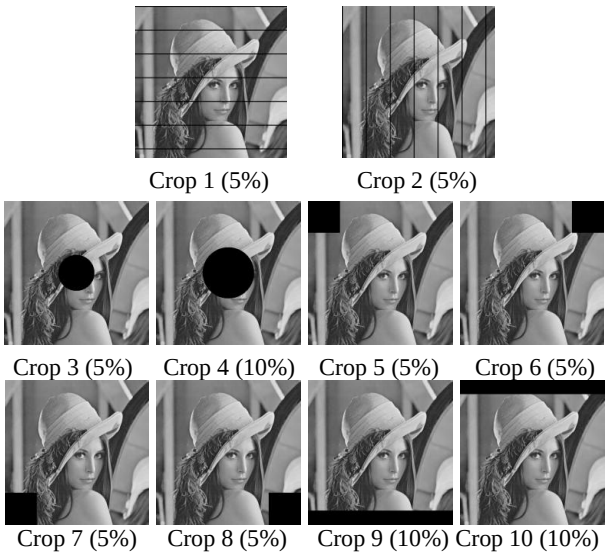
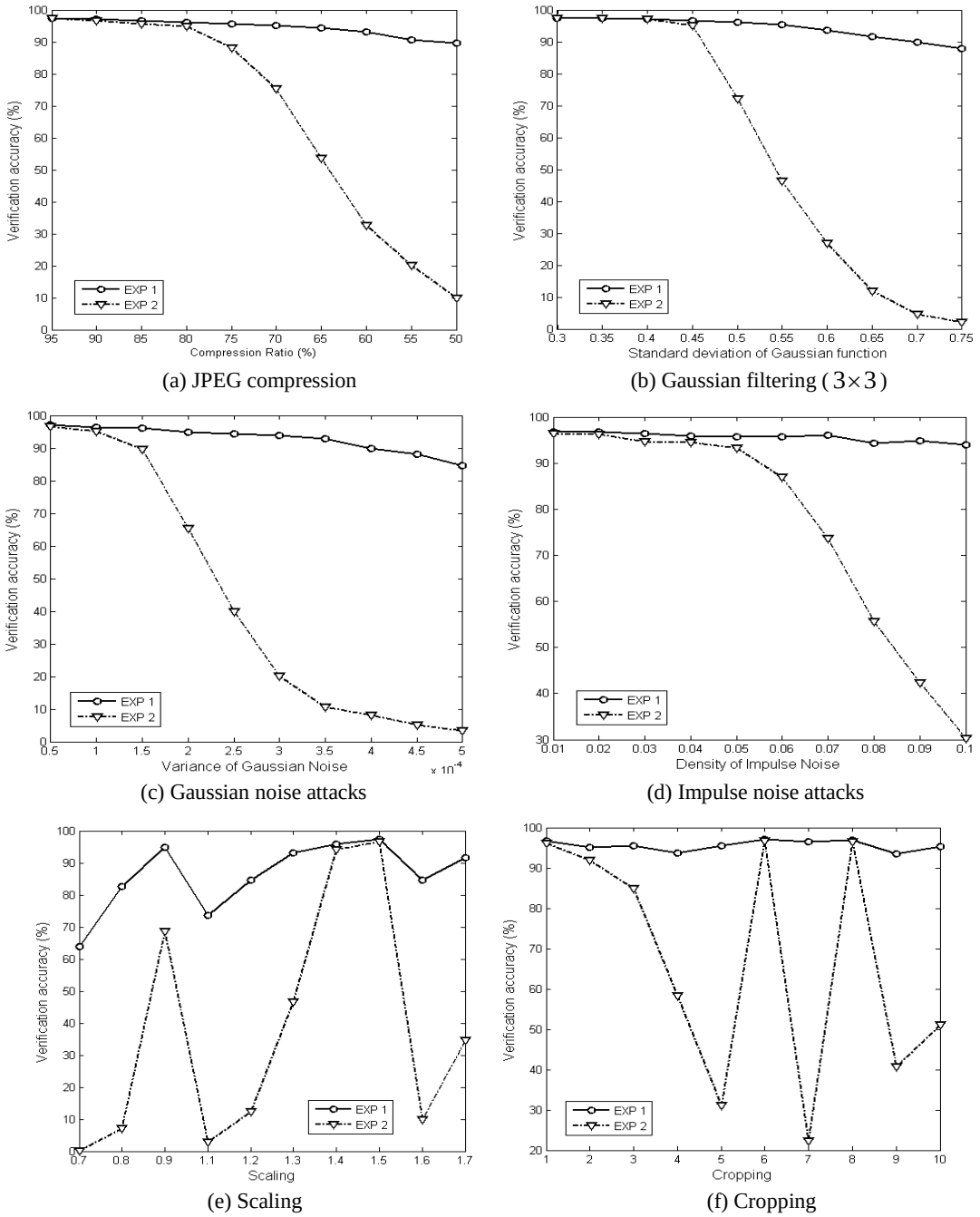


Fig. 7. Ten types of cropping attacks.

The accuracy curves of EXP 1 and EXP2 are shown in Figure 8, where the x-axis and y-axis represent the attack factor and verification accuracy respectively. As seen from Fig. 8, the accuracy curves of EXP1 are much more stable, and exhibit better verification performance than EXP2. For JPEG compression, it has no effect on the accuracy when the compression ratio is 95%. Moreover, the accuracy curves descend slowly while the compression ratio is more than 80%. With further increase in the compression ratio, the accuracy of EXP2 decreases rapidly, but the accuracy of EXP1 reduces very slowly, and can preserve 95.02% with 70% compression ratio. The varieties of accuracy curves under Gaussian filtering, Gaussian noise and impulse noise attacks are similar with JPEG compression. The accuracy is very close to the original one with small attack factors and decreases with increased attack factors. Note that the accuracy of EXP1 can still keep 94.02% under the impulse noise attack with 0.1 noise density, which is lower than the original one by approximately 3.28%.

Different from the former four attacks, the varieties of verification accuracy curves under scaling and cropping attacks are significantly concussive. Accuracy curves of EXP2 have large magnitude of changes, but EXP1 is relatively stable. For the scaling attack, the changing trends of EXP1 and EXP2 are similar. There are two peak value points with the scaling factor increasing from 0.7 to 1.7. The first point appears when the scaling factor is 0.9, with 94.92% of EXP1 and 68.66% of EXP2. When the scaling factor increases to 1.1, the accuracy drops to 73.57% and 2.80%, respectively. With increasing the scaling factor continuously, the accuracy curves of both approaches show upward trends. When the scaling factor is 1.5, they are close to 97.28% and 96.69 %, respectively.

As seen from Fig. 8(f), cropping area, shape and position impact the accuracy directly. The accuracy is different even with the same cropping area but different shapes and positions. Taking the accuracy curve of EXP1 as an example, for both Crop 3 and Crop 6, the percentage of cropping area is 5%, but the accuracy is 95.53% and 97.12%, respectively. It attributes to the adoption of HVS in the hiding process. In other words, the texture might be non-uniformly distributed such that the quality of the extracted secret image is affected by the cropping position directly.



(a) JPEG compression (b) Gaussian filtering (3×3)

(c) Gaussian noise attacks (d) Impulse noise attacks

(e) Scaling (f) Cropping

Fig. 8. Verification accuracy comparisons of various attacks.

The extensive results demonstrate the overall performance of the proposed hiding approach is resilient to some common attacks, which can still be attributed to the correlation analysis. Since the principal part of palmprint can be reconstructed by original cover image at the receiver end with secret key, it is secure and intact. Only the residual part is hidden into the cover image for transmission and might subject to attacks.

However, the damage to this part has lower effect on the recovery of the palmprint, which ensures the integrity of the palmprint.

4. Conclusion and future work

In this paper, a content-based biometric image hiding approach has been proposed for secure network verification. For this approach, the correlation between biometric image and cover image is first discussed by using PCA and PSO, aiming to make use of the abundant information of cover image to represent the biometric image as much as possible. As a result of correlation analysis, the residual image unrepresented with the cover image is regarded as the secret image and hidden into the cover image combining DWT and HVS model. Due to the randomness of PSO and random selection of cover image, the secret key holds high secrecy and is difficult to be deciphered for information extraction. In fact, for secure transmission, the biometric image is divided into two parts: principal part (reconstructed image by cover image using secret key) and residual part (secret image). Single part obtained by the attacker is useless for misdeed or verification. From the experiment results, the proposed approach holds better real-time, and can provide good stego-image quality by utilizing adequately the content of the cover image. In addition, it is robust against some common attacks, and ensures the secure network-based biometric verification.

In the future, we will utilize the feature of spatial and temporal redundancy to obtain better correlation analysis and hiding performances. In order to enhance the practical applicability, other classical and state-of-art blind hiding algorithms will also be discussed. Furthermore, our approach will be expanded to video hiding.

Acknowledgements

This work is supported by National Nature Science Foundation of China (No. 60773098, No.10871037, No. 11071046), the Key Project of MOE (No. 109052), the Fundamental Research Funds for the Central Universities (No. 10QNJJ004, No. 10JCXK008) and the Science Foundation for Young Teachers of Northeast Normal University (No. 09QNJJ006).

References

1. B. Schneier, The Uses and Abused of Biometrics, *Comm. ACM*, **42** (1999) 136.
2. A.K. Jain, Hiding Biometric Data, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **25** (2003) 1494-1498.
3. C. Blundo, A.D. Santis, M. Naor, Visual cryptography for grey level images, *Information Processing Letters*, **75** (2000) 255-259.
4. J.Z. Zhou, R.G. C. Fang, Y.H. Li, Y.C. Zhang, B. Peng, Parameter optimization of nonlinear grey Bernoulli model using particle swarm optimization, *Applied Mathematics and Computation*, **207** (2009) 292-299.
5. H.M. Liu, J.F. Liu, J.W. Huang, Y.Q. Shi, A Robust DWT-based Blind Data Hiding Algorithm, *IEEE International Symposium on Circuits and Systems*, (2002) 672-675.
6. N.K. Ratha, J.H. Connell, R.M. Bolle, Secure data hiding in wavelet compressed fingerprint images, in *International Multimedia Conference, Proceedings of the 2000 ACM Workshop on Multimedia*, (2000) 127-130.
7. A.K. Jain, U. Uludag, R.L. Hsu, Hiding a face in a fingerprint image, in *Proceeding of the International Conference on Pattern Recognition* **3** (2002) 756-759.
8. B. Gunsel, U. Umut, A.M. Tekalp, Robust watermarking of fingerprint images, *Pattern Recognition*, **35** (2002) 2739-2747.
9. M. Vatsa, R. Singh, P. Mitra, A. Noore, Comparing robustness of watermarking algorithms on biometrics data, in *Proceedings of the Workshop on Biometric Challenges from Theory to Practice-ICPR Workshop*, (2004) 5-8.
10. M. Vatsa, R. Singh, A. Noore, M.M. Houck, Robust biometric image watermarking for fingerprint and face template protection, *IEICE Electronics Express*, **3** (2006) 23-28.
11. M. Vatsa, R. Singh, A. Noore, Feature based RDWT watermarking for multimodal biometric system, *Image and Vision Computing*, **27**(2009) 293-304.
12. A. Noore, R. Singh, M. Vatsa, M. M. Houck, Enhancing security of fingerprints through contextual biometric watermarking, *Forensic Science International*, **169**(2007) 188-194.
13. M.K. Khan, J.S, Zhang, L. Tian, Chaotic secure content-based hidden transmission of biometric templates, *Chaos, Solitons and Fractal*, **32** (2007) 1749-1759.
14. S.L. Li, K.C. Leung, L.M. Cheng, C.K. Chan, A novel image-hiding scheme based on block difference, *Pattern Recognition*, **39** (2006) 1168-1176.
15. R.Z. Wang, Y.D. Tsai, An image-hiding method with high hiding capacity based on best-block matching and k-means clustering, *Pattern Recognition*, **40** (2007) 398-409.
16. W.Y. Kim, H.K. Lee, Multimodal biometric image watermarking using two-stage integrity verification, *Signal Processing*, **89** (2009) 2385-2399.
17. Cheng-Yaw Low, Andrew Beng-Jin Teoh, Connie Tee, Fusion of LSB and DWT Biometric Watermarking Using Offline Handwritten Signature for Copyright Protection, *Lecture Notes In Computer Science*, **5558** (2009)786-795.
18. M. Qi, Y.H. Lu, N. Du, Y.N. Zhang, C.X. Wang, J. Kong, A novel image hiding approach based on correlation

analysis for secure multimodal biometrics, *Journal of Network and Computer Applications*, **33**(2010) 247-257.
19. I.T. Jolliffe, Principal Component Analysis, (*Springer*, New York, 1986).
20. J. Kennedy, R. Eberhart, Particle Swarm Optimization, in *Proceeding of the IEEE International Conference on Neural Network*, (1995) 1942-1948.
21. T.H. Sun, Applying particle swarm optimization algorithm to roundness measurement, *Expert Systems with Application*, **36**(2009) 3428-3438.
22. M.V. Oliveira, R. Schirru, Applying particle swarm optimization algorithm for tuning a neuro-fuzzy inference system for sensor monitoring, *Progress in Nuclear Energy*, **51** (2009) 177-183.
23. W.B. Wang, Q.B. Sun, X.C. Zhao, F.C. Yang, An improved Particle Swarm Optimization Algorithm for QoS-aware Web Service Selection in Service Oriented Communication, *International Journal of Computational Intelligence Systems*, **3**(1) (2010) 18-30.
24. I.S. Lee, W.H. Tsaia, Data hiding in grayscale images by dynamic programming based on a human visual model, *Pattern Recognition*, **42** (2009) 1604-1611.
25. H.M. Liu, J.F. Liu, J.W. Huang, Y.Q. Shi, A Robust DWT-based Blind Data Hiding Algorithm, *IEEE International Symposium on Circuits and Systems*, (2002) 672-675.
26. P.N. Tao, A.M. Eskicioglu, A robust multiple watermarking scheme in the Discrete Wavelet Transform domain, *Proceedings of SPIE*, **5601** (2004) 133-144.
27. C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognition*, **37** (2004) 469-474.
28. Y.Y. Tsai, C.M. Wang, A novel data hiding scheme for color images using a BSP tree, *Journal of System and Software*, **80** (2007) 429-437.
29. Z.Q. Zhao, D.S Huang, W. Jia, Palmprint recognition with 2DPCA+PCA based on modular neural networks, *Neurocomputing*, **71** (2007) 448-454.
30. J. Yang, D. Zhang, A.F. Frangi, J. Y. Yang, Two-dimensional PCA: a new approach to appearance-based face representation and recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **26** (2004) 131-137.
31. F.Y. Shih, S.Y.T. Wu, Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*, **36** (2003) 969-975.
32. T.Y. Lee, S.F. D. Lin, Dual watermark for image tamper detection and recovery, *Pattern Recognition*, **41** (2008) 3497-3506.