VOL. 10, NO. 2, FEBRUARY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A NEW BIOMETRIC TEMPLATE PROTECTION BASED ON SECURE DATA HIDING APPROACH

Emad Taha Khalaf and Norrozila Sulaiman
Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Kuantan, Malaysia
E-Mail: pcc13010@stdmail.ump.edu.my

ABSTRACT

Biometrics is a technology that has been widely used in many official and commercial identification applications. The extracted features from the biometric sample is called biometric template which is used during a biometric authentication process. The security of templates is the critical part of biometric system and one of the most crucial issues in designing a secure system. The proposed approach focused on combining data hiding and biometrics to take advantage of the benefits of both fields and develop the hiding technique to find a secure solution for protecting biometric data. We deal with dental as a first biometric source and a user's speech as a second biometric source at same time it a reliable key from a user's speech for enhanced the security of the system. Two of the popular methods are combined DWT and DCT in the proposed security system (SDHA) for embedding and extraction the secret data in order to compensate the drawbacks of both of them and to make the hidden information much more secure against the attacks, Wavelet Transform which use Dyadic Filters to decompose cover image into 4-Levels (HH, HL, LH and LL) and Discrete Cosine Transforms to convert a signal of the selected coefficients (HH, HL and LH) into elementary frequency components. Simply the proposed hiding method are summarized by dividing the secret data into three sections according to the percentages that have been entered by a user then distribute these sections into the three chosen coefficient sets (HH,HL and LH) of the cover image which is an excellent secure locations for data hiding. The results show the efficiency of the proposed method comparing with other method that used skin tone region of images, DWT method and simple LSB method.

Keywords: biometric, template security, data hiding.

INTRODUCTION

A biometric considered as a pattern recognition problem which is uses to identify authorized person based on specific physiological or behavioral features (Preeti and Rajni, 2014). Biometric field has taken a huge interest by global industry with protect and safeguard information as an everlasting necessity, industry has engaged with academic and research institutions in the goal to standardized biometric formats and traits (Group, I. B., 2014). Moreover, revenues in this field are increasing year after year as shown in Figure-1. Most of the current biometric systems employ a single biometric trait this kind of biometric system called unimodel, while the system that employs more than one trait is called multibiometrics (Aly *et al*., 2013). Examples of behavioral characteristics are gait, signature, and voice. Physical characteristics include: DNA, ear, face, fingerprint, hand geometry, iris, and retina (Griaule Biometrics, 2012). The biometric sources like dental, fingerprint, face, iris etc. are captured by the sensor, salient features are extracted using some feature transformation technique and get converted into digital form. This digital information is stored in the database which is known as Biometric Template. Later the template is used during authentication purpose, compromised biometric templates are unlike passwords and tokens they cannot be revoked and reissued this led to become biometric template security is an important issue and protecting the template is a challenging task due to intra user variability in the acquired biometric traits, based on knowledge of the biometric characteristics (Malhotra and Dr. Kant, 2013). A solution to this problem presented here that beside dental template, the secret data is also tagged which is secret by applying steganography technique, so besides enhance user convenience and boost security; it is also protected to various types of threats (Shejul and Kulkarni, 2011). A typical biometric system comprises of several modules. The sensor module acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template.

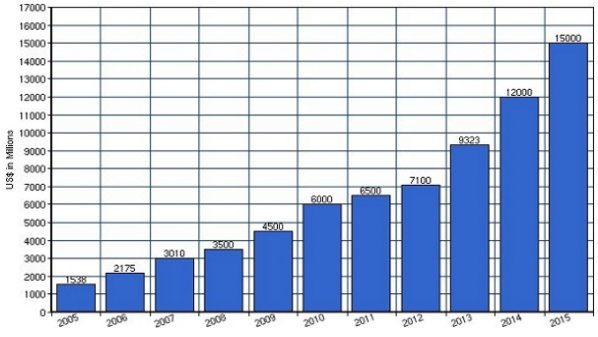


Figure-1. Source: Biometric research group.

Steganography not only hiding the confidential message but also making the hackers believe that the source is clean and they cannot even realize that it contains some hidden information. The purposed system transform domain techniques have been used to address

the limitations of spatial domain and to take advantage of the special properties of alternate domains. Two of the transform domain techniques have been combined wavelet and cosine transform to embed data, by combining the two common frequency methods to take their benefits. The password that have been generated from user's voice which is unique characteristic used then as a condition key to extract the feature vectors of the dental biometric in order to increases the security of the proposed system.

Related work

The biometric authentication systems can be exposed to different attacks, (Ratha *et al*., 2001) have grouped the biometric template attacks into eight classes, and also (Jain *et al*. 2008) have classified these attacks that can be repeated into four categories. Many techniques have been proposed to keep the security of biometric data; one of the suggested techniques was by (Jain *et al*., 2003) with two scenarios of hiding data, first one in a cover image not related to the template data, other scenario by using the fingerprint image to hiding the facial information. (Wang *et al*., 2010) and (Pravin *et al*., 2011) use DCT transformation method to hiding the iris code and the secret information after encrypting in random blocks of the coefficients. Another security system have been proposed by (Klimis *et al*., 2011) based on DWT transformation method to hides biometric signals in video objects over open network.one of the common methods is uses skin region of the image for embedded the template data (Kharge *et al*, 2013), HSV color space has been used to detect skin color tone, also DWT is used to embedded in one of the high frequency sub-band by tracing the number of skin pixels in that band, then cropped a region of the image which will be used as a key at the decoder side (Amritha and Meethu, 2013). A Classical Least Significant bit Technique (LSB) introduced earlier steganography schemes in the spatial domain which directly embed the secret data within the pixels of the cover image (Macq and Quisquater, 1995). This approach has few disadvantages like the relative easiness to implement it makes the method popular, the proper cover image required to hide a secret message inside an image (Wilson and bryon, 1992). Many previous stenographic algorithms have been used pixel domain, its provides the space (capacity), reliability, and controllability in encoding/decoding while embedding the hidden message, but more of the steganalysis attacks will focus on this domain as expected. (Kumar and Shunmugananthan, 2010), (Ramani *et al*., 2008) studied the steganography in transform domain since the compress of digital data will be provides a reduction of storage space and transmission cost.

Biometrics with data hiding

An enhanced data hiding technique has been combined with Biometric to provide stronger security system. Data hiding algorithm has been developed by used both DWT and DCT transforms methods. Biometric key binding is a promising approach to the proposed system in which the biometric template and the key are coupled to form what is known as biometric lock (luels and Wattenberg, 1999) and can retrieval of a digital key using a user's speech as a unique biometric information, This system has been implemented in MATLAB 8.1 using image processing, statistic toolboxes, Microsoft Picture Manager and Photoshop image editing software. Enrollment and authentication process of biometric and data hiding shown in Figure-2 and Figure-3:

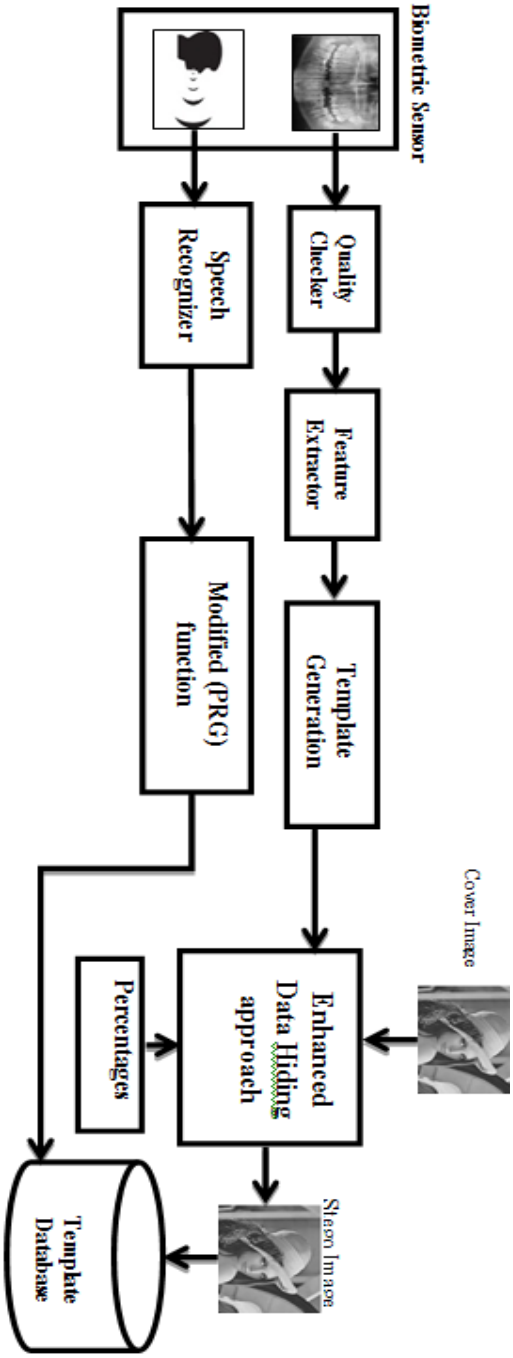


Figure-2. Enrollment process of biometric steganography.

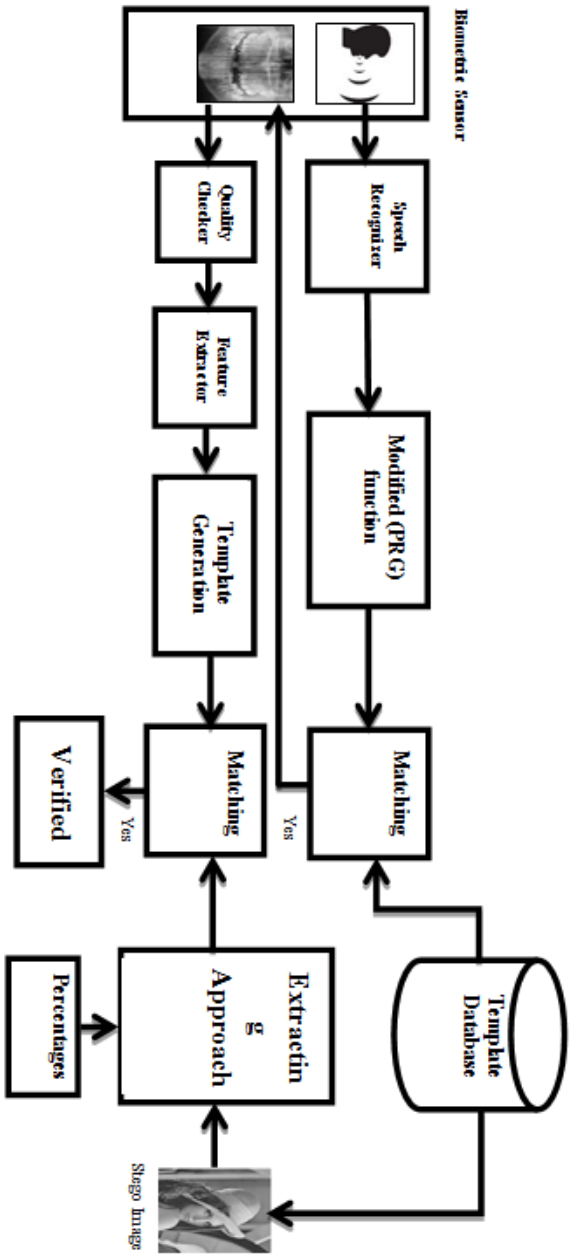


Figure-3. Authentication process of biometric steganography.

Generating the Biometric key

Crypto biometric systems require a secret key or a password which must be tied to an individual through an identifier. This identifier indeed could be a globally unique user id or biometric data. A secret key in our proposed method is a condition to extract the hidden dental template in order to complete the matching process. Human voice provides a unique characteristic which are always there, it can be a good and unguessable by attacker. The generating method is done by applying speech recognition to recognize the password spoken, the generated password is unsecure because the best recognizers can only recognize up to 104 words under best circumstances. Monrose has been use a device as a solution for this problem by repeated utterance of the same password by the same user to improve the security of the key after successful matches with previous recorded utterances (Monrose *et al*., 2001) (Monrose *et al*., 2001). In our proposed method the biometric key that generated from user's voice is used by Pseudo Random Generator (PRG) function to generate a random key; this function generates a different key each time. So, we reset programmatically the default seed before using it in order to have same key in the extract process.

The proposed embedding approach

In the proposed data hiding method the DWT and DCT transforms have been combaned (DWCT) to hide biometric feature vectors. The Wavelet filters decompose the image into a set of non-overlapping multi-resolution sub-bands coefficients which can be reassembled later to reconstruct the original image without error. The 2-D filters divide the 2-D images into four sub-bands HH, HL, LH and LL, as shown in Figure-4.
LL - Lower resolution version of image
HL - Vertical edge data
LH - Horizontal edge data
HH - Diagonal edge data

Data can be embedded effectively by using DWT it will be very suitable to identify the areas in the cover image, due to its excellent "spatio-frequency" localization properties. The coefficient sets can be down sampled without loss of the image information because the bandwidth of the coefficient sets for the resulting sub-bands are smaller than that of the original image. In particular, the property of the masking effect of the human visual system can be exploitation by only modified the DWT coefficient of the region corresponding. In general, in the lower frequency coefficient sets LLx is concentrated the most image energy. So, hiding in this coefficient sets could increase robustness but at same time may degrade the image significantly. On the other hand, changing in the high frequency coefficient sets HHx will not be generally sensitive by the human eye where it includes the edges and textures of the image. This allow to embedding data without being perceived by the human eye. The method of hiding data in the middle frequency coefficient sets HLX and LHX of the image is better in perspective of imperceptibility and robustness (Al-Haj, 2007).

The Discrete Wavelet Transform (DWT) Dilations and translations of the "Mother function," or "analyzing wavelet" Φ(x) define an orthogonal basis, the wavelet basis is:

$$\Phi_{(s,l)}(x) = 2^{-s/2}\Phi(2^{-5}x - l) \quad (1)$$

Where: s and l are integers that scale and dilate the mother function Φ(x) to generate wavelets. The scale index s indicates the wavelet's width, and the location index l gives its position. Notice that the mother functions are rescaled, or "dilated" by powers of two, and translated by integers (Graps, 1995). What makes wavelet bases especially interesting is the self-similarity caused by the scales and dilations. To span the data domain at different resolutions, the analyzing wavelet is used in a scaling equation:

$$W(x) = \sum_{k=-1}^{N-2} (-1)^k c_{k+1} \Phi(2x+k) \quad (2)$$

Where: $W(x)$ is the scaling function for the mother function $\Phi(x)$, and Cx are the wavelet coefficients.

The wavelet coefficients must satisfy linear and quadratic constraints of the form

$$\sum_{k=0}^{N-1} c_k = 2 \quad , \quad \sum_{k=0}^{N-1} c_k c_{k+2l} = 2\delta_{1,0} \quad (3)$$

Where δ is the delta function and l is the location index.

After decompose the cover image into sub-bands, The DCT transform will be applied on the selected sub-bands. The discrete cosine transform (DCT) is used to decompose the image data into parts (or spectral sub-band) of different importance (depending on the image). The DCT is similar to the discrete Fourier transform. It transforms a signal from the spatial domain to the frequency domain (Jeong *et al*., 2005). DCT transform does not affect the input image size, i.e. if the input image is of size ($n \times m$), the output image will be of the same size. DCT transform is often used in compression technique because it tends to concentrate image information. The two-dimensional DCT equations can be expressed as follows:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} Cos\left(\frac{\pi(2m+1)p}{2M}\right) Cos\left(\frac{\pi(2n+1)q}{2N}\right) \quad (4)$$

Where

B_{pq} = The element of the output image

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & p=0 \\ \frac{\sqrt{2}}{\sqrt{M}} & 1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & q=0 \\ \frac{\sqrt{2}}{\sqrt{N}} & 0 \le q \le N-1 \end{cases}$$

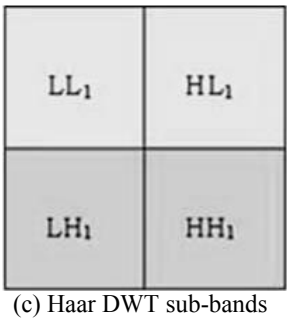
Original image can be reconstructed by applying the following equation of the inverse of discreet cosine transform (DCT-1) (Khayam, 2003):

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q \; B_{pq} \; Cos\frac{\pi(2\pi+1)p}{2m} \; Cos\frac{\pi(2n+1)q}{2n} \quad (5)$$

$$where \qquad 0 \le m \le M-1 \quad , \quad 0 \le n \le N-1$$

In the proposed technique, information has been embedding through reparation technique in frequency domain based on combination of two transforms discrete wavelet transform (DWT) and discrete cosine transform (DCT). Frequency domain steganography is very secure and more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations. It is more secure than spatial domain steganography because information can be spread out to entire image.

(a) Original image (b) After Haar DWT



(c) Haar DWT sub-bands

Figure-4. Lena image before and after one Haar wavelet transform.

Embedding processes

First step before starting embedding is entered the dental image and extract the feature vectors of the biometric resource to generate the template. Second step is receiving the user speech as a password which is converted to random key using the modified Pseudo Random Generator (PRG) function and stored in the template data base. The Embedding process then starts by applying 1-level 2D Haar DWT on the host image then perform the block base DCT with selecting DWT coefficient sets (HH, LH and LH)) and embed data in

middle frequencies in each sub-band depending in percentages entered by the user. Embedding data in the sub-bands (HH, LH and LH) is better in perspective of security and quality. Besides, distribute data in these sub-bands depending on the percentages and non-specific number of bits in each pixel, this will provide confidentiality for embedded data. The processes of embedding data are represented in Figure-5 followed by a detailed explanation.

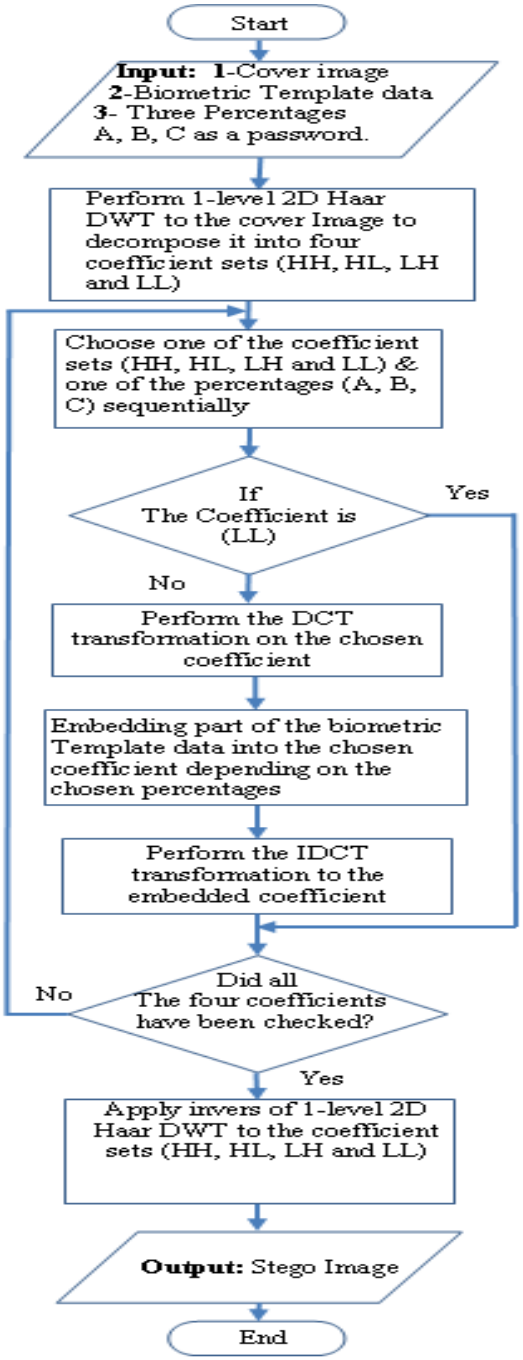


Figure-5. Embedding processes based DWCT.

Input: Stego image, the percentages
Output: The Biometric template data

Step-1: perform DWT on Stego image to decompose it into four non overlapping multi-resolution coefficient sets: HH, HL, LH and LL.

Step-2: perform DCT on the chosen coefficient sets (HH, HL and LH).

Step-3: Process of extracting is start by extracting the total length of the template data vector from the first twenty bits of the coefficient sets, after that compute the lengths of each of the three data bits sets that have been distributed in the three coefficient sets (HH, HL and LH) using the entered percentages.

Step-4: by using the numbers of bits per pixel that have been used for embedding which is agreed between sender and receiver, the embedded data bits are extracted from the LSBs of the coefficient sets (HH, HL and LH).

Step-5: reconstruct the biometric template from the extracted data bits.

ANALYSIS OF CONCEALMENT

The peak signal to noise ratio (PSNR) is introduced (Lu and Liao, 2001), (Yuzhong *et al*, 2004) to evaluate the performance of the proposed scheme and image quality which is defined as:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB \quad (6)$$

$$MSE = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\frac{(a_{i,j} - b_{i,j})^2}{w \times h} \quad (7)$$

Where

$w \times h$ is the image size
ai,j and bi,j are the corresponding pixel values of two images

The PSNR is often expressed on a logarithmic scale in decibels (dB). A larger PSNR value means stego-image preserves the original image quality better. In general, the distortion of the stego image that caused by the embedding can be obvious when the PSNR values falling below 30 dB, while the stego image considered high quality when PSNR value is 40 dB and above (Cheddad, *et al*, 2008). Different sizes of images have been experimented. Figure-6 shows the difference of PSNR when using different sizes of cover images and (1338424) bits as amount of data.

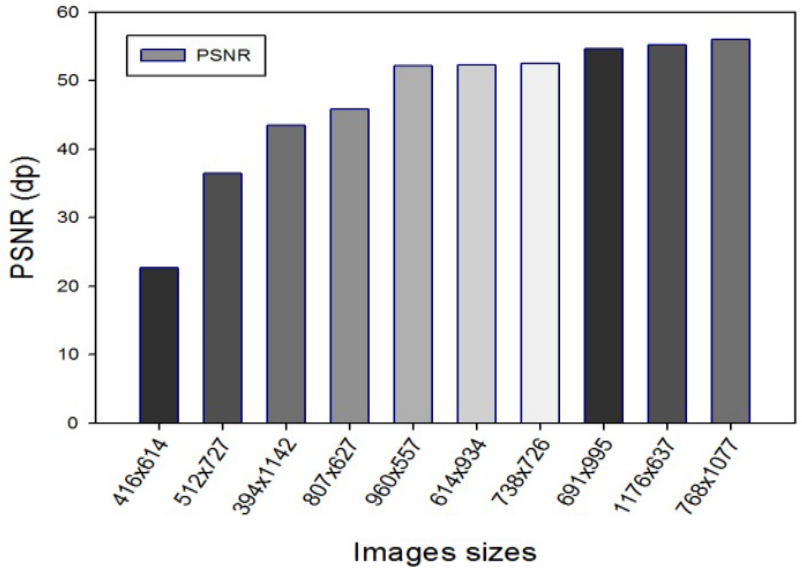


Figure-6. PSNR results for different images sizes.

Table-1. Results of the comparison with the standard LSB and the other methods.

Images	**Size** (bit)	**PSNR**			
		Adaptive LSB	**DWT only**	**Skin tone Stegano.**	**proposed method**
Image 1	776420	38.13	41.85	40.65	45.71
Image 2	747850	38.29	38.36	39.88	39.16
Image 3	780250	38.11	31.69	35.29	41.46
Image 4	770558	38.16	39.32	40.95	41.30

Obviously, hiding data with a good security key is preferable. This is due to the fact that the attacker can't recover the hidden data without getting that key. Chosen percentages which distribute the message bits in the sub-bands will be the key between the sender the receiver. So attacker will not know the amount of data in each sub-band nor even the number of bits used to hide. It should be noted that chosen percentages will determine the quality of the stego image, Table-2 explains the effect of changing the percentages to stego image quality using different images (size of images are 256x256 while the embedded data size was 15% of cover image).

Table-2. Capacity and quality of images using different percentages.

Percentages [HL , LH , HH]	PSNR					
	Lena	CM	Barbara	Peppers	Baboon	Jet
[10%,45%,45%]	52.46	51.06	48.61	47.14	49.51	46.4
[40%,20%,40%]	59.4	55.72	54.44	52.69	53.77	53.3
[35%,30%,35%]	57.38	54.62	53.58	51.04	53.19	51.1
[45%,45%,10%]	51.94	49.24	49.87	45.18	48.5	45.33
[25%,25%,50%]	56.38	53.99	50.27	51.84	51.17	51.3
[20%,20%,60%]	57.66	55.51	50.3	55.47	51.71	54.01

Capacity of the image is also depends on the nature of the image which is varies from image to another. Figure-7 shows the difference of capacity between three images have same size 512x512.

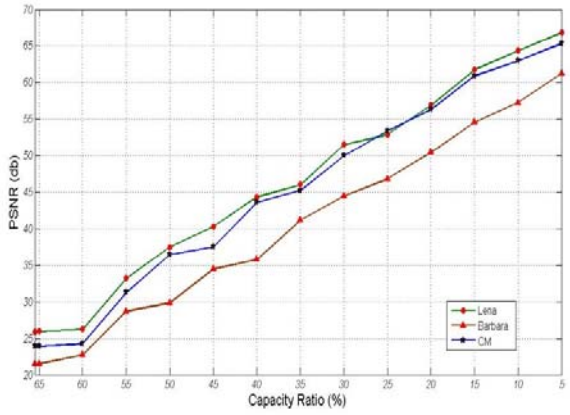


Figure-7. Difference of capacity of three images.

The proposed method has been compared other methods, one of the common methods is uses skin region of the image for embedded the template data (Kharge *et al*, 2013), (Amritha and Meethu, 2013). Other slandered method is the adaptive LSB method (ADLSB); it is enhancing to the classic LSB. As well, proposed method has been compared with a method uses the same proposed technique but with using DWT transform only. The comparison is shown in Table-1.

CONCLUSIONS

In this paper, a new approach of hiding template data has been proposed with combine the hiding system with multi-factor biometric. The results of the proposed hiding system showed high efficiency comparing with other methods, the cover image still maintains a high quality and low PSNR even with large amount of data inside, It also shows an efficiency with all kinds of images, the proposed approach provides good security and protection against any stego attacks, Where the cover image resolution doesn't change much and is negligible besides the key (percentages values) which helps to hide data in unpredictable places in the cover image. On the other hand the random key which is generated from the user's sound gives an extra protection to the system because it became a condition to extract the hidden data of the second biometric (dental) inside the stego image.

REFERENCE

Preeti and Rajni. 2014. Physical Security: A Biometric Approach. International Journal of Engineering And Computer Science. 3(2): 3864-3868.

Group I. B. 2014. www.biometricgroup.com. Retrieved May 12th.

Aly O. M., Salama G. I., Mahmoud T. A. and Onsi H. M. A Multimodal Biometric Recognition system using feature fusion based on PSO. International Journal of Advanced Research in Computer and Communication Engineering. 2(11): 4336-4343.

Griaule Biometrics. 2012. Book-Understanding Biometrics.

Malhotra S. and Dr. Kant C. 2013. A Novel Approach for securing Biometric Template. Internal Journal of Advanced Research in Computer Science and Software Engineering. 3(5): 397-403.

Shejul A. A. and Kulkarni U. L. 2011. A Secure Skin Tone based Steganography Using Wavelet Transform. International Journal of Computer Theory and Engineering. 3(1): 1793-8201.

Macq B.M. and Quisquater J.J. 1995. Cryptology for Digital TV Broadcasting. Proceedings of the IEEE. 83(6): 944-957.

Wilson V. and bryon. 1992. Linear, color separable human visual system model for vector diffusioning system. Journal of Electronic Imaging. 1: 277-292.

Kumar P.M. and Shunmugananthan K.L. 2010. A Multilayered architecture for hiding executable files in 3D images. International Journal of Computer Science and Technology. 3(4): 402-407.

Ramani K., Prasad E.V., Varadarajan S. and Subramanyam A. 2008. A Robust Watermarking Scheme for Information Hiding. International Conference of Advanced Computing and Communications. pp. 58-64.

Ratha N. K., Connell J. H. and Bolle R. M. 2001. An analysis of minutiae matching strength. In: 3rd International Conference on Audio- and Video-Based Biometric Person Authentication, LNCS 2091, Halmstad. pp. 223-228.

Jain A. K., Nandakumar K. and Nagar A. 2008. Biometric template security. EURASIP Journal on Advances in Signal Processing.

Jain A. K. and Uludag U. 2003. Hiding Biometric Data, IEEE transactions on pattern analysis and machine intelligence. 25(2): 1494-1498.

Wang N., Zhang C., Li X. and Wang Y. 2010. Enhancing IrisFeature Security with Steganography. IEEE conference on Industrial Electronics and Applications. pp. 2233-2237.

Pravin M. S. and Shubhangi S. 2011. Stegano-Crypto System for Enhancing Biometric-Feature Security with RSA. International Conference on Information and Network Technology. pp. 196-200.

Klimis N., Nicolas T. and Athanasios D. 2011. Video-Object Oriented Biometrics Hiding for User Authentication under Error-Prone Transmissions. EURASIP Journal on Information Security. p. 12.

luels A. and Wattenberg M. 1999. A fuzzy commitment scheme. Proceedings of ACM Conference on Computer and Communications Security (CCS). pp. 28-36.

Monrose F., Reiter M. K., Wetzel Q. Li S. 2001. Using voice to generate cryptographic keys, Proc. Of Odyssey, The Speaer Verification Workshop.

Monrose F., Reiter M. K., Wetzel Q., Li S. 2001. Cryptographic key generation from voice, Proc. of the IEEE symposium on Security and Privacy.

Al-Haj A. 2007. Combined DWT-DCT Digital Image Watermarking. Journal of Computer Science. 3(9): 740-746.

Graps A. 1995. An Introduction to Wavelets. IEEE Computational Science and Engineering. 2(2).

Jeong S., Hong S. and Won C.S. 2005. Dual Detection of Watermarks Embedded in the DCT Domain. International Symposium. pp. 103-106.

Khayam S.A. 2003. The Discrete Cosine Transform (DCT): Theory and Application. Information Theory and Coding.

Lu C.-S., Liao H.-Y.M. 2001. Multipurpose watermarking for image authentication and protection. IEEE Transactions on Image Processing. 10(10): 1579-1592.

Yuzhong P., Qin CH., Jian Z. 2004. Fragile watermarking self-embedded authentication algorithm of color image. Computer Engineering and Design. 24(12): 2208-2212.

Cheddad A, Condell JV, Curran K and McKevitt Paul. 2008. Enhancing Steganography in Digital Images. The Fifth Canadian Conference on Computer and Robot Vision. pp. 326-332.

Kharge S.M., Deshpande L.M., Kanade S.S. 2013. A New Approach for Skin tone Based Steganography with Key analysis For Mistreatment Biometrics. International Journal of Engineering and Innovative Technology (IJEIT). 3(5): 61-65.

Amritha G. and Meethu V. 2013. Biometric Steganographic Technique Using DWT and Encryption. International Journal of Advanced Research in Computer Science and Software Engineering. 3(3): 566-572.