INTERNATIONAL JOURNAL OF SOCIAL Sciences and Information Technology
ISSN 2412-0294 www.ijssit.com
http://www.ijssit.com

BIOMETRIC TEMPLATE SECURITY USING IMAGE STEGANOGRAPHY

[1*] **Lilian Madivoli** *madivolil@gmail.com*
[2**] **Professor Wilson Cheruiyot** *wilchery68@gmail.com*
[3***] **Dr. Michael Kimwele** *mkimwele@jkuat.ac.ke*

[1] *School of Computing and Information Technology (SCIT), Jomo Kenyatta University of Agriculture and Technology (JKUAT), Nairobi, 00200, Kenya*

***Abstract*:** *Information security is characterized by three aspects: integrity, confidentiality and availability. Securing authentication information remains an important aspect at present in this current age which is characterized by heavy internet usage. Since there is no central administration of the internet, the number of security threats and attacks on authentication information, authentication systems and information being secured has increased. This paper proposed a mechanism that can be used to protect biometric template information through the use of image steganography.*

Keywords: *Biometrics, Biometric Template Security, Image Steganography, Authentication*

1. Introduction

When users need to gain access to a company's resource, various techniques can be used. The oldest of these techniques are PINS or password but they are prone to be cracked through guess work or brute force dictionary (Laghari et al., 2016). For example, in recent years, user account credentials and login details for Yahoo mail users have been stolen by attackers. The worst of the attack happened in 2013. There is no clear information of the exact source of the attack but in its report, Yahoo stated that a third party database that shared the same credentials was the source with no evidence that the usernames and password were taken directly from their systems. To resolve the threats, Yahoo reset the credentials of affected users (Lyne, 2014) and encouraged those who were not affected to do the same regularly so as to prevent them from being compromised (Rossiter, 2014).

Another technique used is biometric authentication which involves authenticating the user through digitized biological data that is obtained from the use and thus are considered to be stronger authentication mechanisms (Software_AG *et al*., 2008). Although considered better than use of passwords, biometrics is still prone to attacks. Techniques used to secure them include use of cryptography and information hiding techniques.

Cryptographic techniques convert the message into cypher text so that the content of the message are not readable by an attacker. Information hiding techniques on the hand is used to hide the existence of important information in some other medium (Thampi, 2004). The major difference between the two techniques is that an intruder is not able to tell presence of secret information in steganography as it uses security through obscurity (Katzenbeisser & Peticolas, 2000). This paper proposes the use of image steganography to secure biometric template information.

The sections following discusses the other related works and their limitations (Section 2), Section 3 discusses the methodology, Section 4 the results of the proposed method and Section 5 gives conclusion and recommendations for future work.

2. Literature Review

Although biometric systems are considered more reliable than other authentication schemes, they are prone to security threats. Figure 1 shows areas in which biometric authentication systems can be attacked. These are indicated by letters a-g (Aljareh et al., 2016).

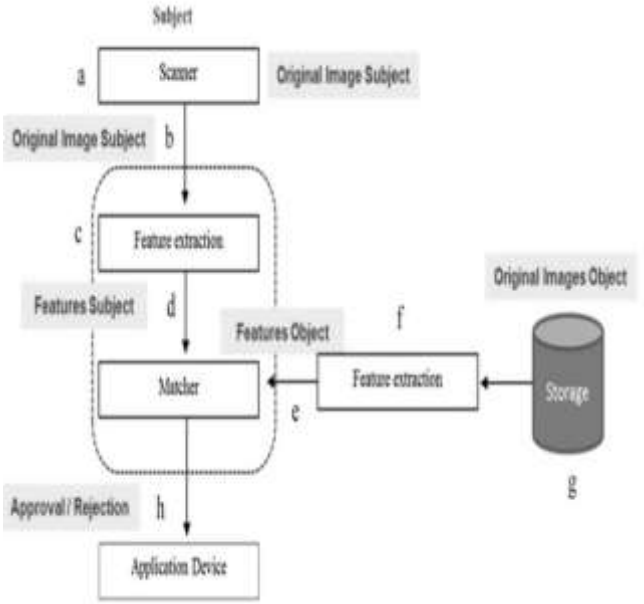

Fig 1 Biometric authentication system attack points.

2.1 Biometric Security Systems

The following sections discuss three types of template protection systems that have been proposed by other research as well as the challenges for each which form the basis of the proposed technique.

2.1.1 Watermarking schemes

(Aljareh *et al.,* 2016) proposed the use of Principal Component Analysis (PCA) and Discrete Coincise Transform (DCT) to protect facial authentication information. Their solution includes a timestamp and a logo as watermarks in facial image. The facial image of a user is captured during an authentication process and compared to one stored in database before a grant access or deny access is made by the system. The captured image is watermarked with a logo (which is a security measure used to compare genuine images from stolen ones) and a timestamp (which is used as a session ID). The disadvantage of these technique is that emphasis was on performance and they neglected perceptibility that is one reason an attacker can use to steal data as they would easily be able to tell that the image contains important information. Also, the time taken to acquire information and authenticate was long for the technique to be implemented in real life.

(Malkhasyan, 2013) proposed a mechanism to protect fingerprints data through the use of steganography. Assume FP_1, FP_2 and FP_C is the first finger, second finger and container respectively that are used during authentication. During an authentication process, FP_1 and FP_2 are scanned. Minutiae points are extracted from FP_2 and are embedded into an extracted fragment of FP_1 as a steganographic algorithm and key. FP_1 is then embedded into FP_C using a steganographic algorithm and key which is is submitted to the server together with the user ID. FP_{1S} is the first finger, FP_{2S} be the second finger, FP_{CS} be the containers that are obtained from the server. Both FP_C and FP_{CS} undergo extraction, in order to obtain FP_2 and FP_{2S} minutia sets which are then compared for integrity and decision is made. FP_1 and FP_{1S} are sets are then extracted from FP_2 and FP_{2S} respectively authenticity decision is made. The limitation of this technique is that the protocol and procedures are complicated.

2.1.2 Cryptographic schemes

As a way to protect against identity fraud in remote authentication, (Narote & Korde, 2015) proposed the use of steganography. In their research, they proposed use of video conferencing where a host's object is extracted. Biometric signal that is captured is undergoes vectorization and is then embedded onto the extracted video object using Qualified Significant Wavelet Tree (QSWT) which is compressed and transmitted. When the stego image

is received, it is decompressed and QSWT is used to detect the biometric templates which are then decrypted for authentication to happen.

Multimodal Biometric-based Secured Authentication System using Steganography (MBSASS), as proposed by (Shanthini & Swamynathan, 2012), used two biometrics, (face and fingerprint), to provide security to the message and authenticates the user indirectly. If two users, say A and B, want to share confidential information, the message is encrypted using the receiver's fingerprint cryptographic key. The sender's face image is then used as a cover image for the encrypted information and header containing the core point, orientation field value and the number of minutiae points of the receiver. The stego image is them divide into a number of portions and scrambled before by the sender before sending it. The receiver then unscrambles the image and uses facial algorithm to verify if the facial image is from a genuine person. If the authentication is positive, the receiver's core point, orientation field value and number of minutiae are compared to that which is contained on the header. If the match is positive, a cryptographic key is generated to decrypt the cipher text in order to get the confidential information. For each communication the users, a different cryptographic key is generated. The limitation of this technique is that the system is complex thus is limited to large organizations.

2.1.3 Multimodal schemes

(Lavanya *et al*., 2012) proposed the use of skin tone region to implement steganography. In their scheme, the secret message is embedded in a cropped region of the image. The cover file first undergoes skin tone detection using HSV (Hue, Saturation and Value) color space using Haar-DWT leading to four sub bands. The payload is then calculated and embedding is done on the high frequency sub bands by tracing the skin pixels in that band. Before performing any of these processes, cropping is done on the cover image and the cropped region is used as a key for both embedding and decoding phases.

(Kant *et al*., 2008) proposed an embedding scheme that involves embedding digital biometrics then transmitting it. During the embedding process, a secret key is embedded in biometric. Their scheme is intended to prevent an imposter from circumvention, repudiation, covert acquisition, collision and coercion. The experimental results for the system are that there is a 49% chance for the message bit to be inserted at pseudorandom location during the first instance, a 50% chance that when message bit is inserted there are no changes in pixel value required and a 12.5% chance that change in pixel value is required if the embedding location is ignored.

In their scheme, (Shejul & Kulkarni, 2010) proposed a method to embed secret data within skin region of image which provides an excellent secure location for data hiding. First the image undergoes cropping which results in an enhanced security than hiding data in the whole image without cropping. The cropped region value is used as a key at decoding side. The second process involves detection of skin tone which is performed using HSV (Hue, Saturation and Value) color space. The cover image is then transformed into frequency domains using Haar-DWT (Discrete Wavelet Transform) which results in four sub bands. Transforming the cover image into frequency domain coefficients assists in identifying information about where vital and non-vital image pixels reside. Payload is then calculated and secret message is embedded in the high frequency sub band of DWT after tracing skin pixels in that sub-band. The image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region. The average Peak-Signal-to-Noise (PSNR) for cropped.

(Goyal & Wang, 2016) used a 2-factor biometric authentication combined with steganography in mobile banking. For a user to login in, they will be needed to provide an eID and password that they were issued with during registration phase. These are verified by the server and it they are correct, they are then redirected to provide the biometrics using their mobile phones to start a video and voice transmission. These two are then hidden in other real life images or videos. The authentication server then receives the login information and decrypts it so as to the information and match it. Data transfer happens if the match is successful.

Multimodal biometrics provide enhanced security as multiple characteristics need to be compared. Such systems would need a real user to be present. The limitation of such systems is that they present extra need to protect user's data.

3. Methodology

This section briefly discusses the data used, their characteristics as well as their source.

3.1 Data collection

The data that was used during this research comprised of 5 fingerprints from DB1-B, 1 fingerprint and 1 minutiae data set from Efinger database and generated 5 synthetic fingerprints. Data obtained from Efinger was assumed to be the authentication information that needs to be secured hence was embedded into our cover files (synthetic fingerprint and DB1-B fingerprints). Data from Efinger and DB1-B database were randomly selected.

3.1.1 Efinger Data selection

Efinger is a fingerprint verification system and is an open source application available on SourceForge (Sharma & Ranta, 2003). The Efinger project was aimed to match a fingerprint image with one that was already contained in its database that consists of 20 fingerprint images that passed that underwent processing. Both the extracted minutiae points and the fingerprints used to obtain them were stored on to it. In total the database had 20 fingerprint impressions and 20 minutiae data sets. The file size for minutiae used was 2.32kb whereas that of the biometric was 192Kb. Minutiae files were stored in .txt format whereas the biometrics were stored in .bmp formats.

This database was selected because it provided ready available minutiae points and biometrics that were needed thus there would be no need to look for additional software to process the fingerprints in order to obtain the minutiae points thus saving on time. Another benefit is that the application was already working, thus the experiments performed on both the minutiae and biometrics were compared against those that are in its database so as to ensure that a certain level of accuracy is maintained during the evaluation.

3.1.2 DB1-B Data selection

DB1-B was used to obtain the second set of fingerprints as they are readily available and are open to the public for anyone in need of them. DB1-B database is part of fingerprint verification competition (FVC) 2004 database that is a publicly available on the internet for use by researchers. DB1 consists of a database of 80 fingerprints collected using an optical sensor "V300" designed by CrossMatch from 30 participants who were required to give 4 impressions of their fore and middle finger in each of their 3 sessions (Biolab, 2003). Fingerprints contained in DB1-B database were all 300kb in file sizes and .tiff file format.

3.1.3 Synthetic fingerprints data generation

The third set of data that comprised of synthetic biometrics was synthetically generated using the SFinGe application which is an open source program. Some of the benefits of using SFinGe include its ability to create large database fingerprints at no cost (Biolab, 1993). There are

four steps that were involved in the generation as depicted by Fig 2.

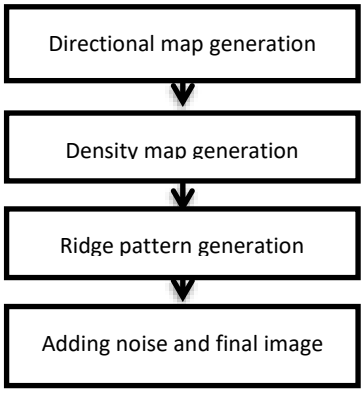

Fig 2 Synthetic fingerprint generation process

Directional map generation started with the positions of cores and deltas and exploited a mathematical flow model to generate a consistent directional map. Density map generation was used to create a density map on the basis of some heuristic criteria. Step C, ridge pattern generation was used to create the ridge-line pattern and the minutiae are created through a space-variant linear filtering. The output of this step is a near-binary very clear fingerprint image.

3.2 Steganography Process

The aim of this research was to secure authentication information in order to ensure that its confidentiality and integrity are maintained. The assumption made through this research was that data (biometric and minutiae) obtained from the EFinger database are the authentication information. These were preferred since, after embedding and decoding of the authentication information, they were then used to verify if the decoded information would match what was in the EFinger database. If a match was found, then the steganography process did not tamper with them.

Image steganography is an open source steganography application used and was obtained from website (Sourceforge, 2011). The application had the capability of embedding both texts and images in files with an option of encryption as well as error reporting capabilities in the event one occurred.

After all data was obtained, the steganography process involved two things: embedding the authentication information and decoding the authentication information as depicted in Fig 3. The research aimed to identify which type of authentication information would be suitable to use as a secret message.

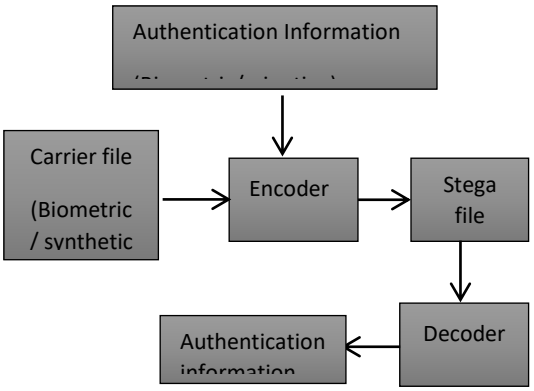

Fig **Error! No text of specified style in document.** Steganography encoding and decoding process

In embedding process, both the authentication information and the carrier files are fed into the image steganography application. These were done by specifying the path location of both files. The final step involved specifying the path location where the stega-file would be stored. Three sets of experiments were done and they involved: Embedding minutia in the cover files, embedding fingerprints in cover files and cropping cover files to check the impact it would have on the steganography process. Eight experiments were conducted on each cover file. In total twenty four experiments were conducted. During the decoding process, path location of the stega-file is specified then one had to choose if the authentication was to

be output as a file or a text. If file option is selected, a path location of where authentication information will be stored is provided. If text option is selected, the information is displayed on the application.

4. Results and Analysis

This section discuss the results obtained from the experiments conducted and analyzed them. File size specified in tables is in Kilobyte and time is in minutes.

4.1 Set A Experiments: Embedding minutia in the cover files

This involved concealing minutia data in the two cover files. The process started off by generation of synthetic fingerprints using the SFinGe which is an open source program. On average, it took 2.64 min to generate one fingerprint and a set of five fingerprints were generated. These together with other five fingerprints from DB1-B that were randomly selected were used in this experiment. In total ten experiments were used to evaluate the performance of concealing minutia in synthetic fingerprint as compared to DB1-B fingerprints.

Table 1 and Table 2 give a summary of the results obtained for synthetic and DB1-B respectively. As indicated in Table 1 and Table 2, generate refers to time taken to create the synthetic fingerprint, embed refers to the time taken to conceal / hide the authentication information in order to secure it and decode refers to the time taken to extract the authentication information from the cover file.

Table 1: Results for embedding minutiae in synthetic fingerprints

SET A1: SYNTHETIC FINGERPRINT				
		GENERATE	EMBED	DECODE
TRIAL ONE	TIME	2.69	0.323	0.282
	FILE SIZE	228	241	2.32
TRIAL TWO	TIME	2.81	0.193	0.157
	FILE SIZE	228	254	2.32
TRIAL THREE	TIME	2.91	0.292	0.193
	FILE SIZE	228	225	2.32
TRAIL FOUR	TIME	2.28	0.238	0.173
	FILE SIZE	228	206	2.32
TRIAL FIVE	TIME	2.51	0.155	0.27
	FILE SIZE	228	252	2.32
AVG	TIME	2.64	0.2402	0.215
	FILE SIZE	228	235.6	2.32

Table 2: Results for embedding minutiae in DB1-B fingerprints

SET A2: DB1-B FINGERPRINT				
		GENERATE	EMBED	DECODE
TRIAL ONE	TIME		0.413	0.288
	FILE SIZE	300	60.1	2.32
TRIAL TWO	TIME		0.392	0.365
	FILE SIZE	300	69.7	2.32
TRIAL THREE	TIME		0.315	0.192
	FILE SIZE	300	75.1	2.32
TRAIL FOUR	TIME		0.475	0.193
	FILE SIZE	300	79	2.32
TRIAL FIVE	TIME		0.425	0.232
	FILE SIZE	300	82.5	2.32
AVG	TIME		0.404	0.254
	FILE SIZE	300	73.28	2.32

Analysis

In this category of experiment, the file size for synthetic fingerprint was 228 on average whereas that of DB1-B was 200kb. Although the

authentication information (minutiae) concealed on both was of the same size, the final size of DB1-B was smaller compared to that of the synthetic fingerprint. Assumption made was that this could have been attributed to the file type i.e. .tiff for DB1-B fingerprints. Future research can be done in this area to identify the impact of file type in a steganography process. It was noted that, the time taken to embed and decode was lesser by 0.164min and 0.039min respectively in the use synthetic fingerprints.

4.2 Set B Experiments: Embedding fingerprints in cover files

This experiment involved concealing biometric authentication fingerprint in the two cover files (Synthetic and DB1-B fingerprints). Since the data was already available for both types of cover files, no generation was required. In total ten experiments were used to evaluate the performance of concealing a biometric image in synthetic fingerprint as compared to DB1-B fingerprints. The average file size for the cover files for both the synthetic and DB1-B fingerprints were 228Kb and 300Kb respectively. Table 3 gives a summary of results obtained for synthetic fingerprints and Table 4 give a summary of the results obtained for DB1-B.

SET B1: SYNTHETIC FINGERPRINT			
		EMBED	**DECODE**
TRIAL ONE	TIME	0.447	0.015
	FILE SIZE	778	193
TRIAL TWO	TIME	0.463	0.275
	FILE SIZE	755	193
TRIAL THREE	TIME	0.193	0.162
	FILE SIZE	746	193
TRAIL FOUR	TIME	0.192	0.172
	FILE SIZE	658	193
TRIAL FIVE	TIME	0.188	0.232
	FILE SIZE	780	193
AVERAGE	**TIME**	0.2966	0.1712
	FILE SIZE	743.4	193

Table 4: Results for embedding biometric fingerprint in DB1-B fingerprints

SET B2: DB1-B FINGERPRINT			
		EMBED	**DECODE**
TRIAL ONE	TIME	0.448	0.123
	FILE SIZE	291	193
TRIAL TWO	TIME	0.33	0.22
	FILE SIZE	315	193
TRIAL THREE	TIME	0.312	0.223
	FILE SIZE	338	193
TRAIL FOUR	TIME	0.197	0.213
	FILE SIZE	344	193
TRIAL FIVE	TIME	0.273	0.243
	FILE SIZE	351	193
AVERAGE	**TIME**	**0.312**	**0.2044**
	FILE SIZE	**327.8**	**193**

Analysis

In Set B experiments, the file size for both types of cover files increased. The final carrier file was 743.3kb for synthetic fingerprint and 327.8kb for DB1-B. The increase was 69.33% in synthetic fingerprint and 38.98% in DB1-B fingerprint. It was also noted that for the case of DB1-B fingerprints, the images had to be pre-scaled in-order for the biometric fingerprint to be embedded. Similarly to Set A experiment, use of synthetic fingerprints as cover files was faster in the steganography process by 0.0154min for the embedding process and 0.0332min for the decoding process.

4.3 Set C Experiments: Embedding fingerprints in cover files

When the experiments were conducted, it was noted that use of synthetic fingerprints to conceal either of the authentication information took lesser time than use of DB1-B fingerprints. Detailed analysis of this is discussed in subsequent subtopic. As a result of the analysis, the research introduced a third set of experiment, Set C, in order to determine the impact of reducing the amount of noise / unnecessary background information on the steganography process. Unwanted section of the

cover files was cropped using Microsoft office picture manager. These experiment was as well conducted for both types of authentication information (minutiae and biometric). Table 5 and Table 6 give a summary of the results obtained for concealing minutiae and biometric information in cropped synthetic fingerprints respectively.

Table 5: Results for embedding minutiae in cropped synthetic fingerprints

SET C1: MINUTIAE				
		GENERATE	EMBED	DECODE
TRIAL ONE	TIME	0.65	0.44	0.39
	FILE SIZE	383	388	2.32
TRIAL TWO	TIME	0.55	0.19	0.35
	FILE SIZE	278	119	2.32
TRIAL THREE	TIME	0.93	0.59	0.4
	FILE SIZE	349	147	2.32
TRAIL FOUR	TIME	0.73	0.56	0.39
	FILE SIZE	244	108	2.32
TRIAL FIVE	TIME	0.7	0.55	0.38
	FILE SIZE	331	136	2.32
AVG	TIME	0.712	0.466	0.382
	FILE SIZE	317	179.6	2.32

Table 6: Results for embedding biometric in cropped synthetic fingerprints

SET C2: BIOMETRIC				
		GENERATE	EMBED	DECODE
TRIAL ONE	TIME	0.65	0.38	0.288
	FILE SIZE	383	592	2.32
TRIAL TWO	TIME	0.55	-	-
	FILE SIZE	278	-	-
TRIAL THREE	TIME	0.93	0.19	0.192
	FILE SIZE	349	620	2.32
TRAIL FOUR	TIME	0.73	-	-
	FILE SIZE	244	-	-
TRIAL FIVE	TIME	0.7	0.26	0.232
	FILE SIZE	331	578	2.32
AVG	TIME	0.712	0.277	0.237
	FILE SIZE	317	596.7	2.32

Analysis

From the Set A and Set B analysis, it was noted that using synthetic fingerprint was more efficient that use of DB1-B fingerprints. This resulted in Set C to be conducted to evaluate the impact of cropping the synthetic images would have on the steganography process for both types of authentication information. On average, it took 0.712min to crop out the unwanted regions from the synthetic fingerprints. This resulted to an increase of the file size from 228kb on average to 317kb on average which is 39.04% increase. In this experiment, the embedding process took more time, on average 0.189min more, in minutiae than in the biometric fingerprints. The decoding process also took 0.145min more for synthetic than DB1-B fingerprints. Although this was the case, it was also noted that for the case of biometric fingerprints, some of the cover files could be used to hide them even after pre-scaling.

4.2 Comparative analysis

The research proposed the use of image steganography to secure biometric information that is used to authenticate users. Section 2.4 gives a summary of some of the proposed techniques used to secure biometrics. Although not much research was found to use synthetic fingerprints, the research borrowed the concept of using steganography from other researches. The following sections compares this research to others in the same in the same field.

Complexity of the model

Techniques proposed by (Malkhasyan, 2013) used two biometrics. In these techniques only one biometric is used for authentication and the other ones are used for watermarking the authentication information in the case of (Malkhasyan, 2013) and for generating cryptographic key for encrypting the biometric used for authentication in the case of (Shanthini & Swamynathan, 2012). Although these two techniques do not have the challenge of fusing the two types of biometrics, as in the case of

multimodal biometric authentication system, the proposed procedures and protocols are complicated and as such are only suited for small organizations that need high end security measures. When compared to these techniques, this research has provided a simple mechanism to secure biometric authentication information that can be implanted in both small and large organizations. In cases where, the maximum security is needed, the method can be improved by use of cryptographic techniques.

Overall time taken

(Aljareh *et al*., 2016) proposed the use of two watermarking scheme to secure authentication information and (Torres *et al*., 2015) proposed the use of two keys to encrypt and decrypt the authentication information. Authentication in the techniques used by (Torres et al., 2015) used encrypted biometric to authenticate users. For both techniques, the overall time taken to authenticate the user was long, as much as 10min, for the techniques to be used in real systems. For this research, the overall time taken to generate synthetic fingerprint, secure the biometrics was 2.64min. Assuming that it took around 1 min to capture the biometric, the overall time would be 3.64min which is less than what the above techniques used.

Need to protect authentication information and cover file

(Linu & Anilkumar, 2012) proposed the use of real fingerprints to secure authentication information. The challenge of using the real biometrics as a carrier file is that one would also have to protect the carrier file as well which in (Linu & Anilkumar, 2012) is not the case. Using synthetic fingerprint image to carry actual fingerprint minutiae data provides an increased level of security since the person who intercepts the communication channel and obtains the carrier image is likely to treat this synthetic image as real fingerprint image.

5 Conclusion

Allowing an authorized user to access information is an important issue as well as is the security and integrity of the authentication information used during an authentication process. Use of minutiae to be embedded in a cover file through the use of steganography can be assumed to be more efficient as compared to using biometrics. This is clearly shown by the lesser time taken to hide and extract them. Using synthetic fingerprints as a cover file is beneficial as an intruder would easily mistake them as the actual fingerprint. Thus the need to protect both the authentication information and the cover file was addressed by this research. The performance of the model was measured on the time taken to generate, embed and decode as well as accuracy of extracting the authentication information which was 100%. Therefore the research showed that, besides securing authentication information through use of steganography, errors relating to wrong authentication would not arise as all the information needed for authentication is not lost in the process. Future research can be conducted to evaluate the impact a file type, in this case for the cover file, has on the steganography process.

References

Aljareh, S., Yusoff, Z., & Yusoff, Z. (2016). A watermarking technique to improve the security level in face recognition systems. Springer, 23805–23833.

Biolab. (1993). biolab.csr.unibo.it/sfinge.html. Retrieved from biolab.csr.unibo.it: http://biolab.csr.unibo.it/sfinge.html

Biolab. (2003). Fingerprint Verification Competition. Retrieved from Fingerprint

Verification Competition: http://bias.csr.unibo.it/fvc2004/

Goyal, D., & Wang, S. (2016). Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems. ResearchGate, 1-5.

Kant, C., Nath, R., & Chaudhary, S. (2008). Biometrics Security using Steganography. International Journal of Security, 1-5.

Katzenbeisser, S., & Peticolas, F. A. (2000). Information Hiding Techniques for Steganography and Digital Watermarking.

Laghari, A., Waheed-ur-RehmaN, & Memon, Z. A. (2016). Biometric authentication technique using smartphone sensor. Islamabad, Pakistan: International Bhurban Conference on Applied Sciences and Technology (IBCAST).

Lavanya, N., Manjula, V., & Rao, N. K. (2012). Robust and Secure Data Hiding in Image Using Biometric Technique. International Journal of Computer Science and Information Technology, 5133-5136.

Linu, P., & Anilkumar, M. N. (2012). Authentication for Online Voting Using Steganography and Biometrics. . International Journal of Advanced Research in Computer Engineering & Technology, 26-32.

Lyne, J. (2014, January). http://www.forbes.com/. Retrieved from http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/#423349215b49: http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/#423349215b49

Malkhasyan, N. (2013). Authentication based on Fingerprint with Steganographic Data Protection. International Journal "Information Theories and Application, 289-294.

Rossiter, J. (2014, January). http://yahoo.tumblr.com/. Retrieved from http://yahoo.tumblr.com/post/750835323112/important-security-update-for-yahoo-mail-users: http://yahoo.tumblr.com/post/750835323112/important-security-update-for-yahoo-mail-users

Shanthini, B., & Swamynathan, S. (2012). Journal of Computer Science. Multimodal Biometric-based Secured Authentication System using Steganography, 1012-1021.

Sharma, S., & Ranta, S. M. (2003). efinger.sourceforge.net/index_files/v3_document.html. Retrieved from efinger.sourceforge.net: efinger.sourceforge.net/index_files/v3_document.html

Shejul, A. A., & Kulkarni, P. U. (2010). A DWT based Approach for Steganography Using Biometrics. International Conference on Data Storage and Data Engineering, 39-43.

Software_AG; Planet; News_Phone. (2008). ICT Standards: Database Security Guide.

Sourceforge. (2011, February 25). sourceforge.net/projects/image-steg/?source=navbar. Retrieved from sourceforge.net: https://sourceforge.net/projects/image-steg/?source=navbar

Thampi, S. (2004). Information Hiding Techniques. India.

Torres, W. A., Bhattacharjee, N., & Srinivasan, B. (2015). Privacy-preserving biometrics authentication systems using fully homomorphic encryption. International Journal of Pervasive Computing and Communications, 151-168.

Wei, Q., Zhu, H., Lu, R., & Lu, H. (2017). Achieve Efficient and Privacy-preserving Online Fingerprint Authentication over Encrypted Outsource Data. IEEE ICC 2017 Communication and Information System Security Symposium. Paris, France: IEEE