International Journal of Software Engineering and Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 4 Issue 1, pp. 120-132, February 2018
©Universiti Malaysia Pahang
https://doi.org/10.15282/ijsecs.4.1.2018.10.0043

FINGERPRINT WATERMARKING WITH TAMPER LOCALIZATION AND EXACT RECOVERY USING MULTI-LEVEL AUTHENTICATION

Wei Keat Lee, Siau Chuin Liew
Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang, 26300 Gambang, Kuantan,
Pahang Darul Makmur, Malaysia
Email: weikeat94.lwk@gmail.com

ABSTRACT

This paper presents the tamper localization and exact recovery using multi-level authentication in fingerprint watermarking. The proposed scheme will be detecting the tampered sector of fingerprint images when the watermark is embedded in the original image. If the sector has been tampered, the sector will be able to recover the original data. Furthermore, exact pixel value of the fingerprint image is used to embed the feature of extraction and recovery of the original fingerprint image from the tampered image. This paper also describes the usage of SHA-256 as a hash function, the usage of Least Significant Bit (LSB) technique to perform tamper detection, localization and recovery in the Region of Interest (ROI). The proposed scheme does not require original fingerprint for detection on the tampered sector and recovery. It uses 512 x 512 pixels fingerprint images and 288 x 180 pixels of ROI in this study. The experimental results showed that the tamper detection and localization were successfully detected and localized the tampered sector. The tampered sectors were restored accurately and the average peak signal-to-noise ratio (PSNR) value of watermarked image was 44.1518 dB. The experimental result proved the effectiveness of multi-level authentication.

Keywords: Watermarking, Tamper localization, Exact Recovery, Fingerprint image.

INTRODUCTION

Development of science and technology has brought us great convenience and fast-paced life which brought us easily exposed to others. Hence, security is needed to defence ourselves from being attacked or stolen via the technology. Properties such as phone, personal document, pictures, automated teller machine (ATM) card, accessing system, etc. required a high secure protection in order to keep our belonging safe. There are numerous methods to protect those things with high security. One of the protection methods is to use fingerprints to access the application or system. Fingerprints are the tiny ridges, whorls and valley pattern on the tips of each finger. It forms into pressure on a baby’s tiny, developing fingers in the womb. In this world, there are nobody has totally similar fingerprints even the identical twins. In spite of the fact that, identical twins can have same DNA but not the fingerprints. Therefore, fingerprint is a unique and immutability which is even more distinct than Deoxyribonucleic Acid (DNA). There are three main classes of fingerprint: whorl, arch, and loop. A whorl pattern is a circular pattern of around the center of the fingerprint while the arch pattern is a line that starts from one side and ends on the other. The arch pattern does not has delta and core, and it looks like aware. A loop pattern must have one or more ridges entering from one side and then takes a U-turn and comes back to the same side. The center point of these patterns is called the core.

In this work, watermarking was introduced in order to protect the fingerprint data in a database. There are two types of watermarking which are visible watermarking and invisible watermarking. Visible watermark is the watermark which can be viewed by naked eyes meanwhile invisible watermarking is the marking which could not be seen by naked eyes. Invisible watermarking is where information is added to the image data. Some invisible watermarking requires some mathematical calculations to retrieve the actual data. Fundamentally, digital watermarking is a method for embedding some secret key in the original image which can extract or detect for authentication purposed (Preeti & Rajeev, 2014).

Numerous studies were conducted with tamper detection in fingerprint images. However, tamper detection and recovery in fingerprint images was less reported. Jasni and Azma (2006), proposed a watermarking method to embed the watermark data into fingerprint images without corrupting the original features of the fingerprint. The objective for their work is to preserve the original of fingerprint features. The experimental result shows that the second level of detection get nearer 100% of detection. However, this method could not be used for all conditions and this method may cause some tampering left undetected by using average intensity block in authentication watermark checking (Liew & Jasni, 2011). Hence exact pixel method will be used instead of average intensity block method in order to have a 100% recovery of original images. In addition, Liew, Liew and Jasni (2010) presented an algorithm based on Jasni and Abdul (2006) scheme and implemented the multi-level of authentication. This method can prove that multilevel authentication had considerably saved the time taken in the recovery process but certain condition may not detected 100%.

Osamah and Khoo (2010) presented a method to provide a good visual quality of watermarking in a medical image with ROI-based tamper detection and recovery using the reversible watermarking technique. This method is not applicable when the image size is big and the ROI size is big. To overcome this problem, we proposed to used fingerprint image with size 512 x 512 pixels was collect from the Internet with 288 x 180 pixels of ROI portion.

In this study, fingerprint image with size 512 x 512 pixels was collect from the Internet. Tamper detection was used to detect any tampering in the image while tamper localization was used to detect which portion has been tampered. For recovery, it was used to recover the tampered image to the original image. To improve Jasni and Azma (2006) work, tamper detection, localization and recovery watermarking will apply in the fingerprint images to make it more user friendly and flexibility on detecting the fingerprint image and to avoid failure detection or recovery in any level of authentication. To ensure all conditions can detect the tampered section with 100% successful, the exact pixel method will introduce in this research. In order to reduce time taken on detection and recovery, multi-level of authentication will apply in this research as well.

PROPOSED METHOD

In order to enhance previous works of Jasni and Azma (2006), this chapter will explain the methodology of this research. Watermarking is the central section in this research. One of the computationally intensive parts of watermarking with tamper detection and localization capability is processing which included embedding and extraction. In this research, the main object is fingerprint image. The 8bits, 512 x 512 pixels of different type of fingerprint images are selected. A 288 x 180 pixels are defined as region of interest (ROI) was used to store critical information in the fingerprint image. To embed the key information, Least Significant Bit (LSB) was then used for embedding the key information. Exact recovery method was used to recover the tampered image. Multi-level of authentication will be explained for higher flexibility and less time-consumption. In this research, the authentication algorithm has three levels which containing ROI hash function check, single sector hash function check and recovery stage. If first level authentication test is failed, then the second level and third level would be executed further for tampering. Thus, this method would reduce the operating time. From Jasni and Azma (2006) work, they focused on feature of tamper detection in their research only. Therefore, this research focuses on the protection of fingerprint image and recovery information. Liew and Jasni (2011) proved that the usage of average intensity in watermarking may failed in certain conditions and caused some tampering left undetected. Therefore, exact pixel method was used in this work as an authentication watermark. The exact pixel method for fingerprint is very sensitive. The proposed algorithm will be detected if the sector had been tampered as one of the pixels has modified.

Region of Interest

According to Cappelli et al. (2007), ridges and valleys are the main structural characteristic of the fingerprint. Some fingerprint matching algorithms are referring to a core point, generally dedicated to the position of the north most loop uniqueness or as the point of maximum ridgeline curvature for fingerprints belonging to the arch class. The most efficient way to describe the orientation image is the ridgeline pattern. Usually, there are two types is adopted features for the fingerprint matching: termination and bifurcation. Termination is the point where the ridge suddenly stops or terminates while bifurcation is a ridge divides into two ridges (Cappelli et al., 2007). As reported by Chris (2016), minutiae are very specific features to verify. Minutiae are the line our fingerprint terminate or split into two. Therefore, we proposed to use 288 x 180 pixels for ROI portion and the rest are region of non-interest (RONI) portion. The ROI portion is divided into 4 x 4 sectors which consist of 72 x 45 pixels for each sector. Figure 1 shows the sample of images of ROI and RONI portion in the fingerprint image and Figure 2 shows the 4 x 4 sector of ROI portion.

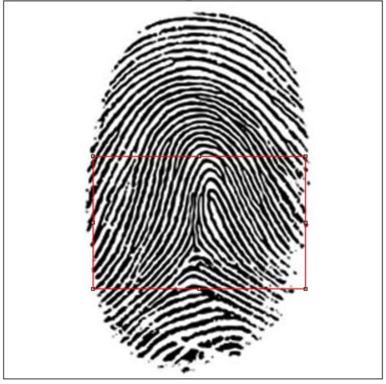


Figure 1 ROI and RONI portion in fingerprint image

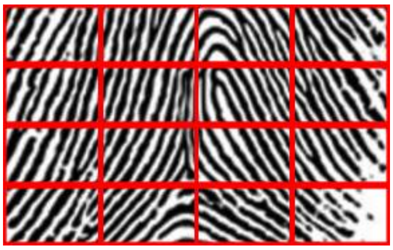


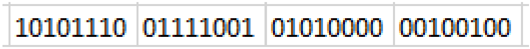
Figure 2 4 x 4 sectors of ROI portion

Hash Function

SHA-256 algorithm is a one-way function which produces an almost-unique and fixed-size 256-bit (32-byte) hash (Swathi & Senthil, 2016). The SHA-256 algorithm has a very similar structure with SHA-1 as it is one of the inheritor hash functions to SHA-1. SHA-256 is the strongest hash function currently available which is more secure and less vulnerable to attacks. SHA-256 was used to hash the ROI portion before embedded into the fingerprint image and extracted image after tampered sector. SHA-256 also applied for each sector after ROI divided into 4 x 4 sectors which are 72 x 45 pixels for each sector. SHA-256 was applied during the detection stage. The value of hash generated in 256 bits was compared to ensure the ROI is not modified. The purpose of SHA-256 application is to increase the security in the fingerprint image.

Least Significant Bit

The term of Least Significant Bit (LSB) plays an important role which shows the smallest bit of the binary sequence. Darshana (2010) used the LSB method to embed watermark in his work. In our work, the two least significant bits for each pixel were used in the RONI portion. Figure 3 shows the 4 pixels in binary value for an image with the watermarked value of 57 (00111001). The watermarked value was split one by one and each of the bits were replaced from the last least significant bit then the second least significant bit and preceded with the second pixels value. Figure 4 shows how each bit replaces the pixel value while the result of watermarked image is illustrated in Figure 5.



10101110	01111001	01010000	00100100

Figure 3 Pixels in binary value for an image

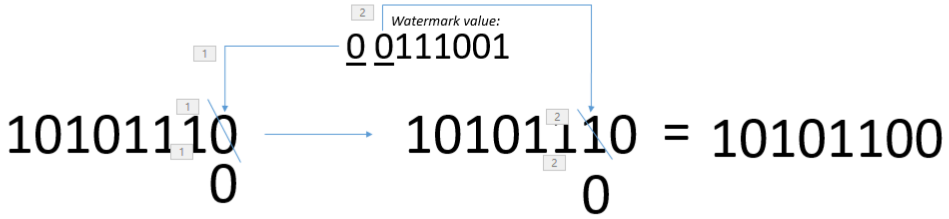
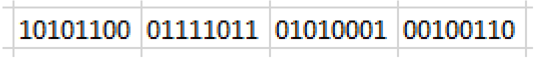


Figure 4 Process of Least Significant Bit



10101100	01111011	01010001	00100110

Figure 5 Result of watermarked image

Image Authentication

According to Liew and Jasni (2011), the tamper localization process will fail in certain conditions and caused some tampering left undetected by using average block intensity in watermark authentication. Therefore, we decide to use exact pixel method with multi-level authentication method as an authentication watermark. In order to protect the primary portion of the fingerprint, 288 x 180 pixels of ROI will be used in this research. The ROI portion will be divided into 4 x 4 sectors. Each sector is 72 x 45 pixels. The authentication bit was computed from the hash value of ROI portion and each sector. The hash value is embedded to the RONI portion with LSB method. In the image tamper detection and localization procedure, there are two main processes as follows:

Embedding process

Embedding process is to embed the information into the image and the information can be extracted and detected later. The embedding process can be described as follows:

i. The fingerprint image is segmented into ROI and RONI portion.
ii. The hash value of ROI portion is calculated by using the SHA-256 hash function.
iii. Calculate the length of hash value.
iv. Retrieve the start point for embedding process.
v. The hash values are embedded into RONI portion with LSB method.
vi. Update the total RONI size used.

Extraction process

The process of watermark extraction shown in following:

i. Get the length of information that going to extract.
ii. Get the start point of extraction.
iii. Extract the last bit of the RONI pixel value.
iv. Extract the second last bit of RONI pixel value.
v. Repeat step (iii) and (iv) till all values has been extracted.

Tamper Detection and Localization

There are two level hierarchical tamper detection and localization schemes in this study. In the level 1 detection, we focus on the ROI portion. If the ROI portion has been tampered, Level 2 detection will be implemented. The level 2 detection is focused on each sector of the ROI portion. Figure 6 shows the flow of Level 1 and Level 2 detection and the Level 1 and Level 2 detection can be illustrated as follows:

Level 1 detection:

i. Determine the ROI and RONI portion.
ii. Calculate the hash value of current ROI portion, *h2.*
iii. Retrieve the start point of retrieve previous ROI hash value.
iv. Extract the ROI hash value from RONI portion, *h1.*
v. Compare *h1* and *h2.*

vi. If *h1=h2*, then end the process; otherwise continue Level 2 detection.

Level 2 detection:

i. Divide the ROI portion into 4 x 4 sectors which are 72 x 45 pixels for each.
ii. Get the start point of each sector hash value from RONI portion.
iii. Retrieve each sector hash value from RONI portion, hSector.
iv. Calculate each current sector hash value, hSector2.
v. Compare hSector and hSector2.
vi. If hSector ≠ hSector2, mark the sector invalid; otherwise, mark it as valid
vii. Repeat step ii to vi till all sectors has been checked.

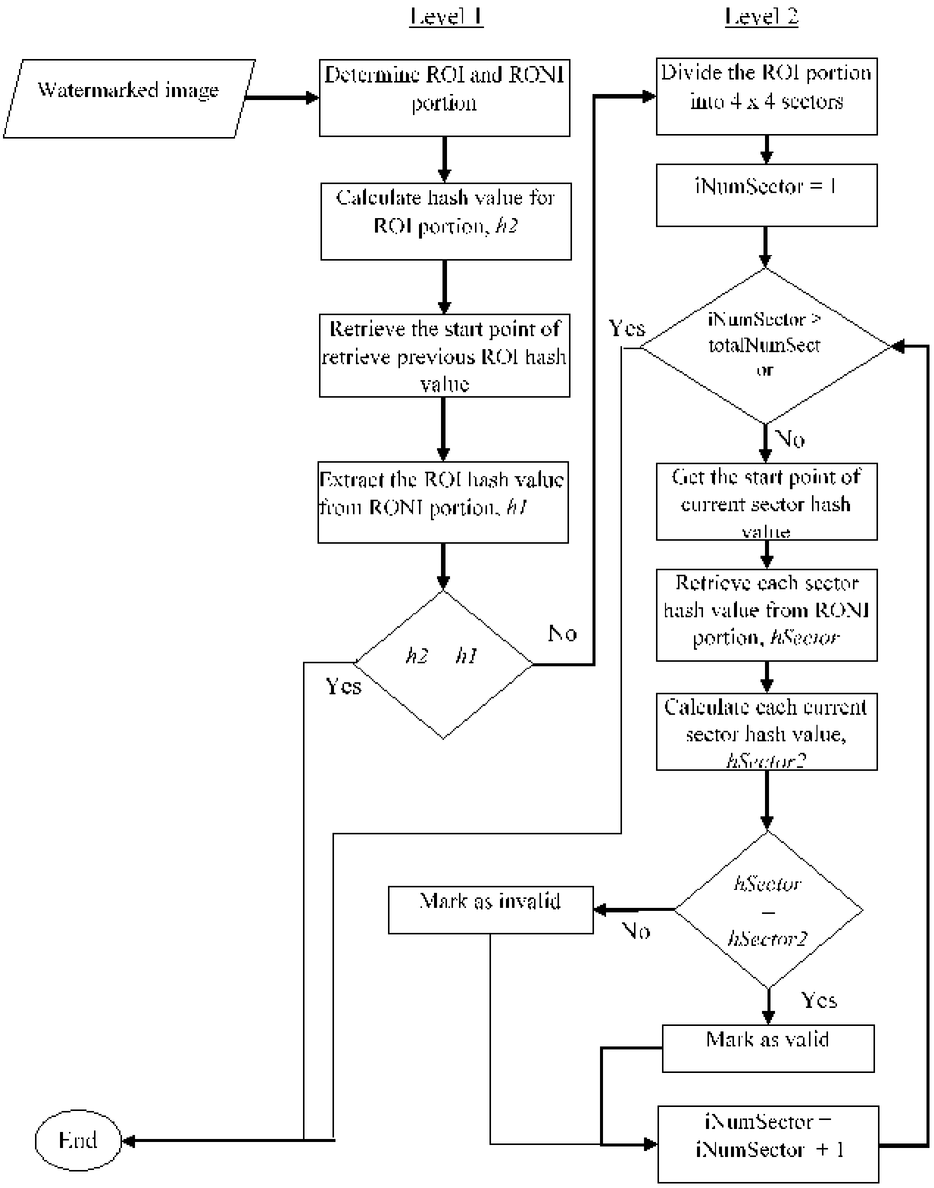

Level 1
Level 2
Watermarked image
Determine ROI and RONI portion
Calculate hash value for ROI portion, *h2*
Retrieve the start point of retrieve previous ROI hash value
Extract the ROI hash value from RONI portion, *h1*
h2 *h1*
No
Yes
Divide the ROI portion into 4 x 4 sectors
iNumSector = 1
iNumSector > totalNumSector
Yes
No
Get the start point of current sector hash value
Retrieve each sector hash value from RONI portion, *hSector*
Calculate each current sector hash value, *hSector2*
hSector = *hSector2*
No
Yes
Mark as invalid
Mark as valid
iNumSector = iNumSector + 1
End

Figure 6 Flow of Level 1 and Level 2 detection

Recovery

After the tamper detection process, all sectors in the image are marked either valid or invalid. Those invalid sectors need to be recovered. Figure 7 shows the flow of recovery process and the recovery process can be elaborated as follows:

i. If the sector is marked as valid, continue with following sector; otherwise, get the start point of the current sector.

ii. Make a new matrix with the same size of sector, *tempSector*.

iii. Retrieve the last two least significant bits from RONI with the start point and put into *tempSector*.

iv. Overlap the current sector with *tempSector*.

v. Repeat step iii and iv till all invalid sectors has been recovered.

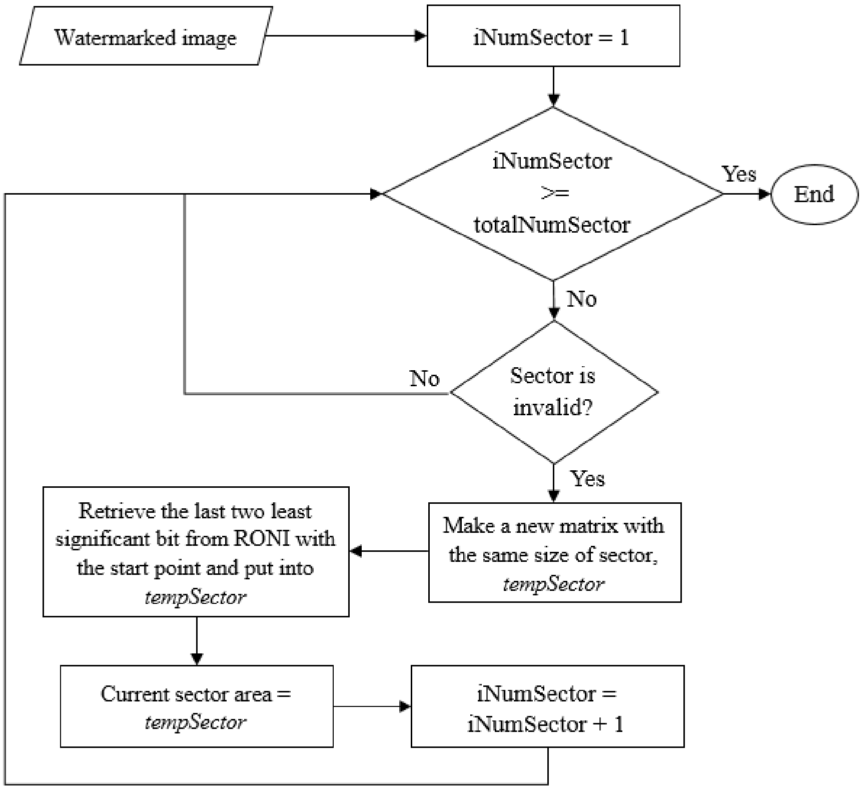

Watermarked image
iNumSector = 1
iNumSector >= totalNumSector
Yes
End
No
Sector is invalid?
No
Yes
Make a new matrix with the same size of sector, tempSector
Retrieve the last two least significant bit from RONI with the start point and put into tempSector
Current sector area = tempSector
iNumSector = iNumSector + 1

Figure 7 Flow of recovery process

EXPERIMENTAL RESULTS AND DISCUSSION

The 8 bits of the 512 x 512 pixels fingerprint images were selected to ensure the message embedding has been carried out. A total of eight experiments were carried out to test the usage of hash function during the embedding and extraction process of the image watermarking. Tamper detection, localization and recovery were also tested. SHA-256 was used as the hash function for all experiments. All experiments carried out with different cover images and different hash values. The hash value depends on the ROI portion. The average PSNR value of watermarked image is 44.1518 dB. In evaluating the proposed watermarking with tamper detection and localization, three types of tampering methods were applied for all experiments which are salt and pepper noise, Gaussian noise and rotation of certain sectors of the cover image. Figure 8, 9, 10 show three sample of the original images, watermarked images, ROI portion, tampering with salt and pepper noise, Gaussian noise and rotation certain sector with -5º. It also shows each tampering method with the ROI portion and recovered image. Three figures proved that those tampering methods are detected and localized successfully in tampering image. Figures 8 (d), 9 (d) and 10 (d) was manipulated using salt and pepper noise while Figures 8 (e), 9 (e) and 10 (e) are the ROI portion of the fingerprint images. Figures 8 (h), 9 (h) and 10 (h) was manipulated using Gaussian noise. Figures 8 (l), 9 (l) and 10 (l) was manipulated using rotation certain sector with -5º. Figure 8 (f), 8 (j), 8 (n), 9 (f), 9 (j), 9 (n), 10 (f), 10 (j) and 10 (n) show the grey colour sectors has been tampered. The tampered sectors were restored accurately in g, k and o. The experimental results also proved that multi-level authentication is effective.

From the figure 8, 9 and 10, the differences between the cover image and watermarked image are hardly identifiable by human eyes. Both images have different value for each pixel, but we still difficult to differentiate the image by using human eyes to view. One of the methods to shows the differences between the cover image and watermarked image is used histogram analysis. Histogram normally refers to a histogram of the pixels intensity values. The histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. Therefore, we can see clearly the differences between original image and watermarked image. PSNR stands for Peak Signal-to-Noise Ratio. It is used to measure the quality of reconstruction of lossy and lossless compression. The range of PSNR in this research is between 42 and 45. Although the PSNR value in this research is slightly lower than Jasni and Azma (2006). It is because we used 209536 totals RONI bits over 210304 total RONI bits. It is means left 768 RONI bits we do not use.

To detect whether the watermarked image has tampered, three different tampering method has been used which are salt and pepper noise, Gaussian noise and rotate certain sector with -5˚. In our proposed method, compare the hash value for the cover image and watermarked image can detect the original image is modified or not. If both hash values are dissimilar, it verifies that watermarked image has tampered. There is two levels detection in our proposed method. In Level 1 detection, it is compared hash value of ROI portion while Level 2 detection is compared hash value of the sector in ROI portion. In Level 2 detection, if the hash values of sector are different, the sector will be masked as invalid. During the detection process, all tampered sectors can successfully detect and localize tampered sector. After tamper detection and localization process, all sectors are marked either valid or invalid. For those invalid sectors need to be recovered. If the sector tampered, then the sector will become grey in colour which is 128 pixel values; otherwise, the sector remains same pixel value. From our proposed algorithm, it can prove that all hash values of ROI portion of recovered image are same with the hash values of the ROI portion of the original image. Therefore, all sectors are successfully recovered by using exact recovered in this research.

The experimental result has apparently shown the advantage of the proposed method as compared to other techniques. In this research, it able to detect all tampered sectors and recovers back to the original sector. Otherwise, the multi-level authentication is performed correctly.

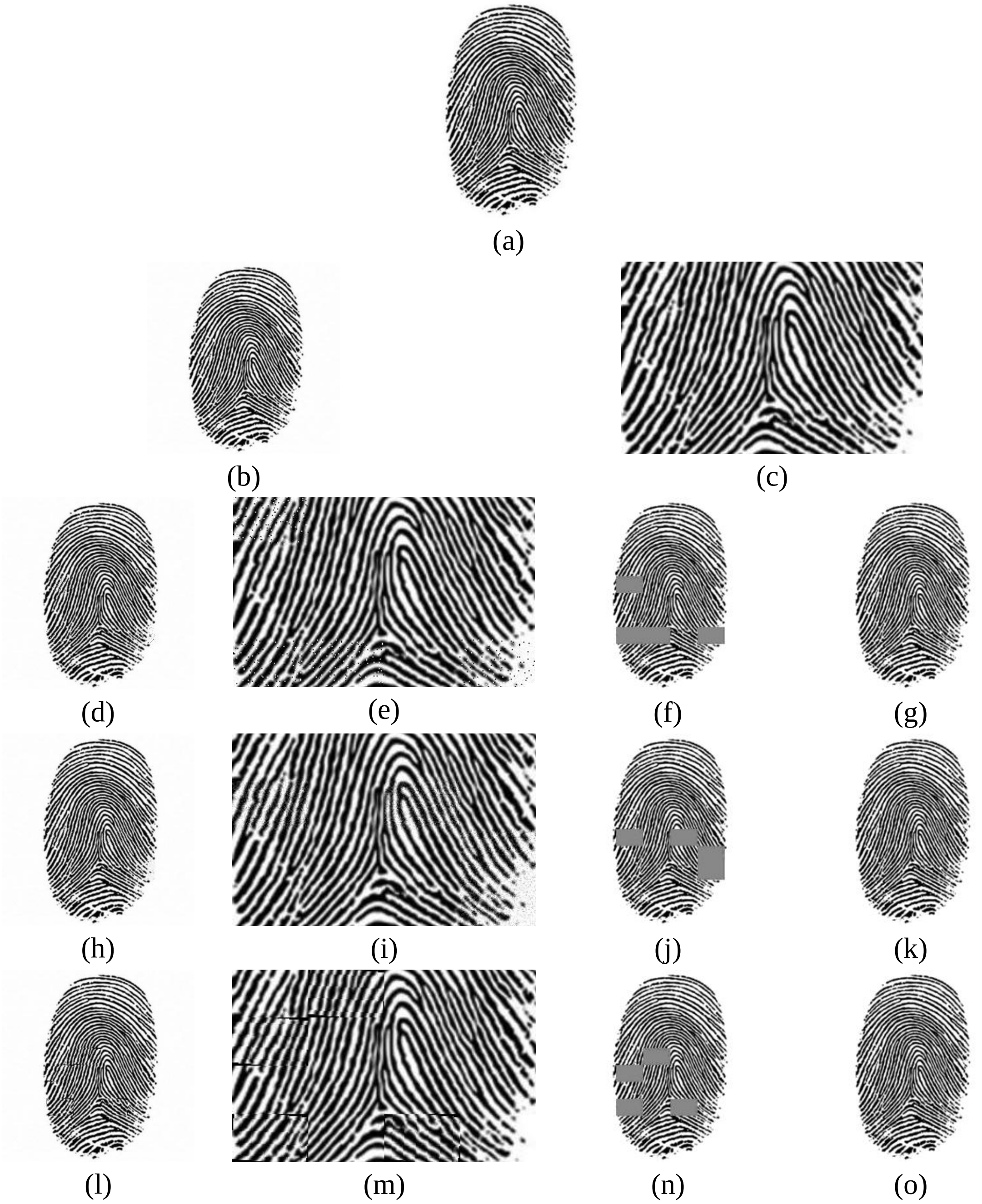


Figure 8(a) Original image (b) watermarked image (c) ROI portion of watermarked image (d) tampered image with salt and pepper noise (e) ROI portion of tampered image with salt and pepper noise (f) detected image (g) recovered image (h) tampered image with Gaussian noise (i) ROI portion of tampered image with Gaussian noise (j) detected image (k) recovered image (l) tampered image with -5˚ rotate certain sectors (m) ROI portion of tampered image with -5˚ rotate certain sectors (n) detected image (o) recovered image

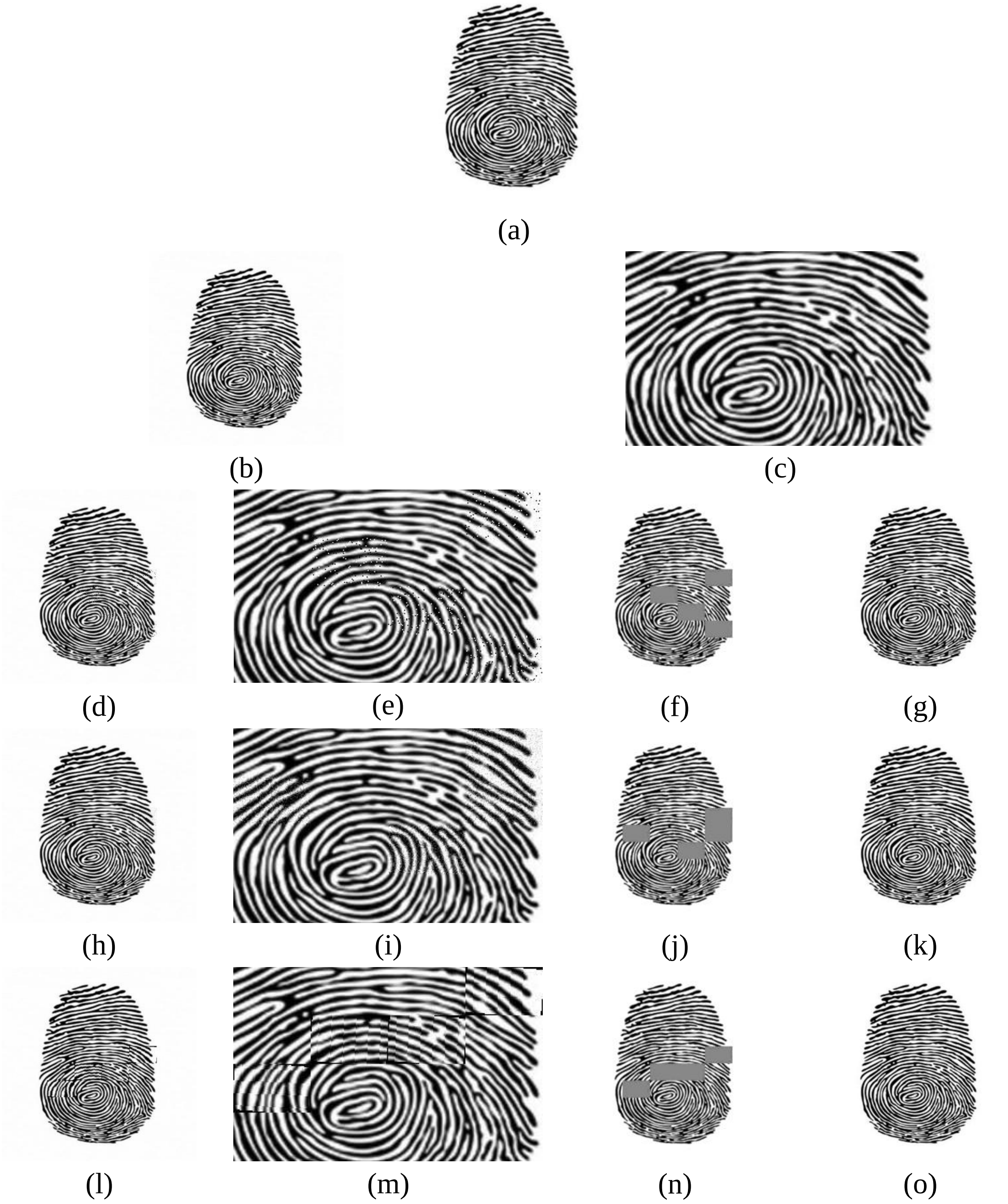


Figure 9 (a) Original image (b) watermarked image (c) ROI portion of watermarked image (d) tampered image with salt and pepper noise (e) ROI portion of tampered image with salt and pepper noise (f) detected image (g) recovered image (h) tampered image with Gaussian noise (i) ROI portion of tampered image with Gaussian noise (j) detected image (k) recovered image (l) tampered image with -5˚ rotate certain sectors (m) ROI portion of tampered image with -5˚ rotate certain sectors (n) detected image (o) recovered image

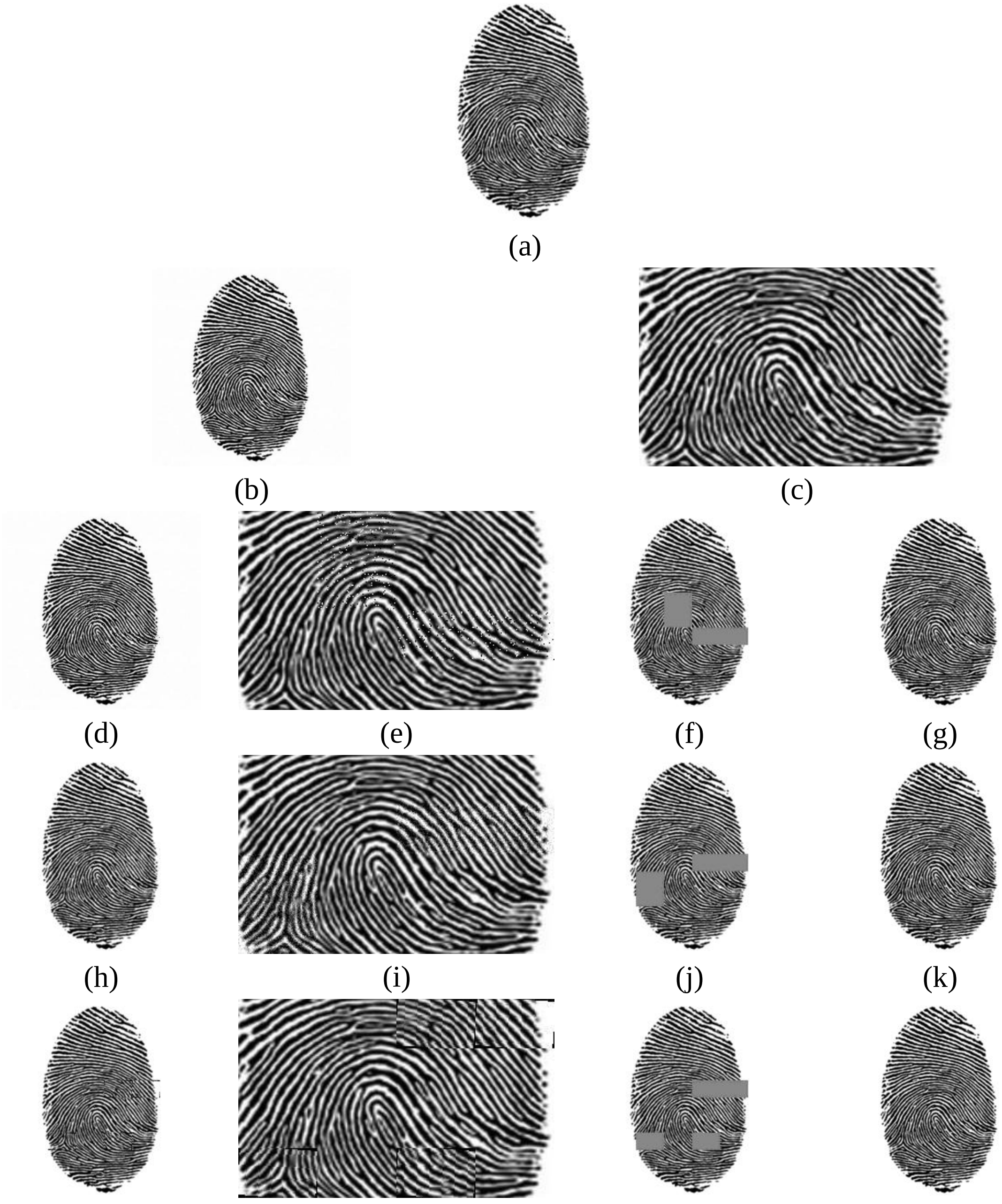


Figure 10 (a) Original image (b) watermarked image (c) ROI portion of watermarked image (d) tampered image with salt and pepper noise (e) ROI portion of tampered image with salt and pepper noise (f) detected image (g) recovered image (h) tampered image with Gaussian noise (i) ROI portion of tampered image with Gaussian noise (j) detected image (k) recovered image (l) tampered image with -5˚ rotate certain sectors (m) ROI portion of tampered image with -5˚ rotate certain sectors (n) detected image (o) recovered image

CONCLUSION

A watermarking method that can detect and localized tampered images as well as recovery was proposed. Therefore, the watermarking procedures in fingerprint images that includes image embedding, image extraction, multilevel detection and exact recovery was successfully conducted and shows good performance in terms of security. The main objective for this research is to protect the fingerprint image and make sure the fingerprint images have high security. Few researchers have done their research with tamper detection in fingerprint images and least of number done with tamper detection and recovery in fingerprint images. Therefore, we introduced our watermarking procedures in fingerprint images that include image embedding, image extraction, multilevel of detection and exact recovery. The experiments show the watermarking procedures can successfully perform well. In this research, the program takes longest time on recovery stage. It is because the program needs to retrieve the pixels from RONI portion one by one and restore into tampered sector. Therefore, a different method of hash function can be used to reduce the size of RONI. Other than that, the program only applicable for 4x4 sectors for maximum sector size. It is because we use exact recovery method which embed which each pixel value into RONI portion and the RONI bit we left is 768 bit. The amount is not enough if we apply for sector. So, flexible ROI area can be carried out. Other than that, the tampered sectors can be increased to reduce time execution and increase the flexibility on detecting.

ACKNOWLEDGEMENT

First of all, I would like to grab hold this golden opportunity to express my sincere thanks to my supervisor, Dr. Eric Liew Siau Chuin for his motivation, advices and guidance to me in the inception to completion of this thesis. Dr. Eric has given me much useful comment in this study. He has always been there whenever I am facing the problem that unable to solve.

Other than that, I would also like to acknowledge my beloved family and my friends for their support and love throughout my life as well as sharing their valuable ideas and knowledge with me.

Last but not least, I would like to thank all lecturers that giving me guidance to completion of this project.

REFERENCES

Cappelli, R., Lumini, A., Maio, D. and Maltoni, D. (2007). Fingerprint image reconstruction from standard templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29, 1489–1503. doi: 10.1109/TPAMI.2007.1087.

Darshana, M. (2010). Comparison of Digital Water Marking methods. *International Journal on Computer Science and Engineering*, 2(9), 2905–2909.

Jasni, M. Z. and Abdul, M. F. (2006). Medical image watermarking with tamper detection and recovery., IEEE Engineering in Medicine and Biology Society. Conference, 3270–3273. doi: 10.1109/IEMBS.2006.260767.

Jasni, M. Z. and Azma, B. A. (2006). Fingerprint Watermarking with Tamper

Detection, *3rd International Conference on Artificial Intelligence in Engineering and Technology*, (1), 1–4.

Liew, S. C., Liew, S. W. and Jasni, M. Z. (2010). Tamper Detection And Recovery With Run Length Encoding Compression, *World Academy of Science, Engineering and Technology*, 48, 799–803

Liew, S. C. and Jasni, M. Z. (2011). The usage of block average intensity in tamper localization for image watermarking, Proceedings - 4th International Congress on Image and Signal Processing, CISP 2011, 2, 1044–1048. doi: 10.1109/CISP.2011.6100301.

Liew, S. C., Liew, S. W. and Jasni, M. Z. (2013). Tamper localization and lossless recovery watermarking scheme with roi segmentation and multilevel authentication, Journal of Digital Imaging, 26, 316–325. doi: 10.1007/s10278-012-9484-4.

Osamah, M. A.-Q. and Khoo, B. E. (2010) ROI-based tamper detection and recovery for medical images using reversible watermarking technique, IEEE International Conference on Information Theory and Information Security ICITIS, 151–155. doi: 10.1109/ICITIS.2010.5688743.

Preeti, P. and Rajeev, K. S. (2014). A Survey: Digital Image Watermarking Techniques, International Journal of Signal Processing, Image Processing and Pattern Recognition, 7(6), 111-124.

Swathi, G. and Senthil, K. M. (2016). Image Watermarking Using Secure Hash Algorithm, International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST), 2 (10), 1393-1399.