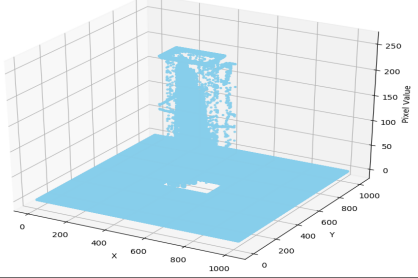
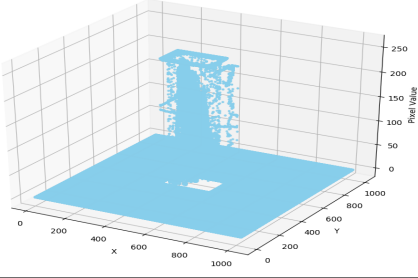
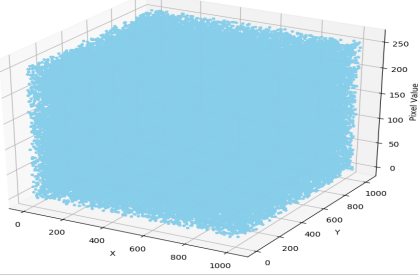
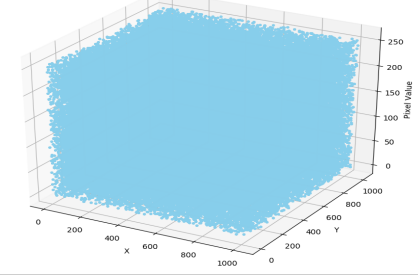
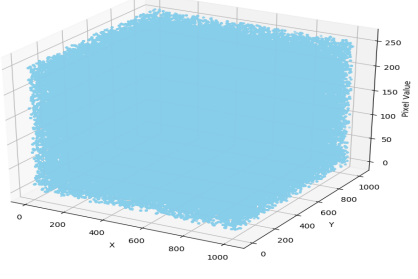
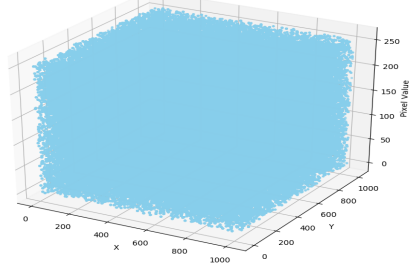
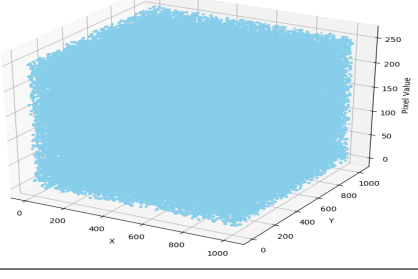
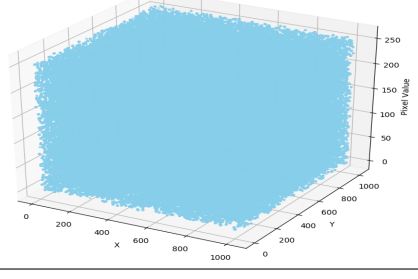


4. Experiment Result and Analysis

In this section, we describe our experiment which consisted of experiment and analysis on image encryption, visual quality, embedding capacity, and security analysis. These experiments used twelve medical images with size of 1024 x 1024 pixels as the test image as shown in Fig.4.

Table 1: Comparison of The Pixel Distribution between Previous and Proposed Method

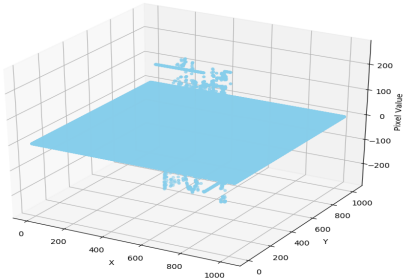
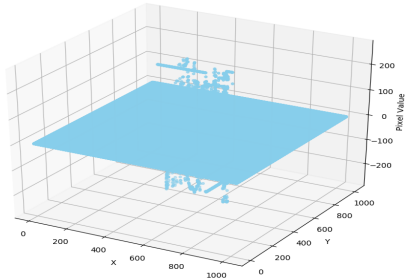
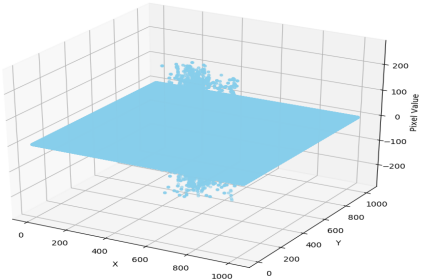
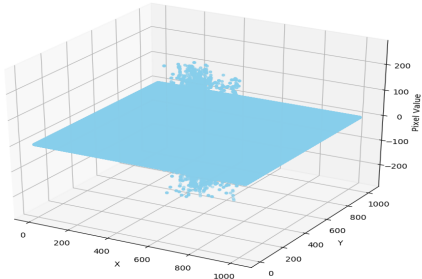
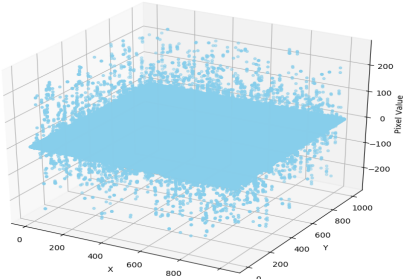
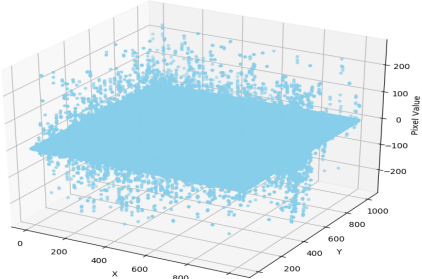
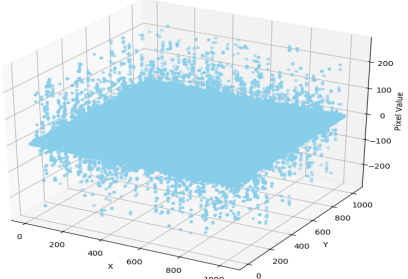
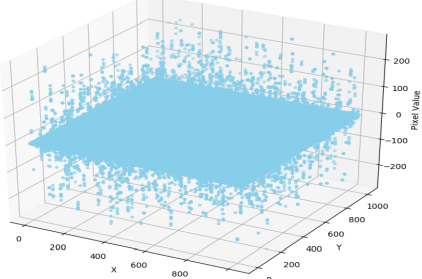
		Previous Method	Proposed Method
Original Image (Image 1)			
			
Permuted Encrypted Image	Session 1		
	Session 2		

4.1. Security Analysis

In implementation of encryption process, the generated key was reused for 9 pixels. So, the encryption process may leak the difference information between the neighboring pixel in the same sub-block. For analyzing the security of the proposed method, we have to calculate the probability of obtaining the secret image. Based on the basic concept of the proposed method, an attacker may obtain the difference value between two pixels if the attacker can intercept

two pixels encrypted with the same key. Thus, for securing the secret message, permutation is applied. However, if the permutation is static, then the key of the permutation can be obtained by the attacker using known plain text attack. To secure our proposed framework, a dynamic permutation algorithm is conducted using Eq.2. To restore the original image, the attacker must restore the original arrangement of the sub-block. For obtaining the encrypted image, the attacker should find the invers of the dynamic permutation. Suppose the probability of a successful known plain text attack on an encryption system is $1 / u$, then using a static permutation the probability of success is $1 / u$. Meanwhile, when using dynamic permutations, the probability of successfully performing a known plain text attack on an encryption system would be $1 / (u.N)!$ or $1/N!$ less than when using static permutations, where N is the number of sub-block. Thus, the security level of the proposed method will increase such that it is greater than the security level of Huang’s method.

Table 2: Comparison of The Pixel Value Difference between Previous and Proposed Method

		Previous Method	Proposed Method
Original Image (Image 1)			
Encrypted Image			
Permuted Encrypted Image	Session 1		
	Session 2		

4.2. Experiment and Performance Analysis of The Proposed Method

This section discusses about the experiment conducted for observing the correlation between neighboring pixels in the encrypted image, the recovered and decrypted image quality, as well as the embedding capacity.

Suppose in session 1 we encrypted image (a), then permuted it using key 1. Based on the proposed method, in the second session we encrypted image (a), then permuted it using another key, while using the previous method, they used key 1 to permute the encrypted image in session 2. The result of encryption and permutation process is shown in Table.2. Based on the difference histogram, it is shown that the correlation between neighboring pixel of encrypted image could be preserved because the pixels are still randomly distributed as shown in Table.2, even we used different permutation. However, the pixel value differences were slightly different between the first and second session. this condition was occurred because of the different permutation. Thus, since the permutation key of each session is unique, then it is harder to obtain the key than using similar key for all session as has been discussed in subsection 4.1.

Table 3: Visual Quality of Recovered Image (PSNR 1) and Decrypted Image Without Message Extraction (PSNR 2)

	DHS1				DHS3			
	Previous Method		Proposed Method		Previous Method		Proposed Method	
	PSNR1	PSNR2	PSNR1	PSNR2	PSNR1	PSNR2	PSNR1	PSNR2
Image 1	69,160	31,680	69,160	31,950	69,160	26,163	69,160	26,408
Image 2	69,196	26,540	69,190	26,520	69,196	25,410	69,196	25,409
Image 3	69,120	26,400	69,129	26,400	69,120	25,420	69,129	25,425
Image 4	69,188	25,220	69,188	25,225	69,188	25,190	69,188	25,194
Image 5	69,118	25,985	69,118	25,989	69,118	25,985	69,118	25,989
Image 6	69,415	28,799	69,415	28,830	69,415	26,801	69,415	26,855
Image 7	69,015	28,210	69,008	28,120	69,015	27,411	69,008	26,480
Image 8	69,290	28,210	69,293	28,330	69,290	25,148	69,293	25,233
Image 9	69,192	28,170	69,198	28,206	69,192	24,000	69,198	25,099
Image 10	69,177	25,996	69,170	25,910	69,177	25,650	69,170	25,612
Image 11	69,210	26,194	69,207	26,104	69,210	25,832	69,207	25,782
Image 12	69,150	25,662	69,157	25,540	69,150	25,100	69,157	25,009

For observing the quality of the decrypted image, we conducted experiment for measuring the peak signal-to-noise ratio (PSNR). The higher PSNR, the closer an image to the original one. In the experiment, we used two messages that have different size to be embedded into the cover image. The first message's size was 160000 bits, while the second one was 640000 bits. The experiment's result is shown in Table.3. PSNR1 measured when the image is decrypted after extracting the secret message, while PSNR2 is measured when the image is decrypted without extracting the secret message. Based on the result, it can be concluded that the PSNR1 using previous and proposed method were similar using our test image, but PSNR2 was different when using the previous and proposed method. This condition is occurred because the permutation used in the previous and proposed method were different. The significant difference was occurred between PSNR1 and PSNR2 using either previous and proposed method. This condition was occurred because the result of image decryption without extracting message will generate noise.

For observing the capacity, we calculate the number of two neighboring pixel whose difference is 0 and -1. In this case, since we used similar cover image for previous and proposed method, then the embedding capacity using those methods are equal. The result is shown in Table.4.

Table 4: The Embedding Capacity (EC) of Example Image

Test Image	Embedding Capacity (bits)		Test Image	Embedding Capacity (bits)	
	Previous Method	Proposed Method		Previous Method	Proposed Method
Image 1	911997	911997	Image 7	614096	614096
Image 2	375320	375320	Image 8	712379	712379
Image 3	381175	381175	Image 9	695552	695552
Image 4	176035	176035	Image 10	289499	289499
Image 5	99713	99713	Image 11	299350	299350
Image 6	686576	686576	Image 12	346925	346925

5. Conclusions

In this paper, we present RDH scheme using encryption and dynamic permutation for strengthening the security against known plain text attack. Based on the experiment result it can be concluded that the proposed method is stronger than previous one while maintaining the correlation between neighboring pixels, as well as the embedding capacity. However, in the proposed method the sender and the receiver should remember the session number before they start the session.

References

1. Ni, Z., Shi, Y.Q., Ansari, N., Su, W.. Reversible data hiding. *IEEE Transactions on circuits and systems for video technology* 2006; **16**(3):354–362.
2. Ramaswamy, R., Arumugam, V.. Lossless data hiding based on histogram modification. *Int Arab J Inf Technol* 2012;**9**(5):445–451.
3. Barton, J.M.. Method and apparatus for embedding authentication information within digital data. 1997. US Patent 5,646,997.
4. Tian, J.. Reversible data embedding using a difference expansion. *IEEE transactions on circuits and systems for video technology* 2003; **13**(8):890–896.
5. Lee, S.K., Suh, Y.H., Ho, Y.S.. Reversible image authentication based on watermarking. In: *Multimedia and Expo, 2006 IEEE International Conference on*. IEEE; 2006, p. 1321–1324.
6. Huang, F., Huang, J., Shi, Y.Q.. New framework for reversible data hiding in encrypted domain. *IEEE Transactions on Information Forensics and Security* 2016;**11**(12):2777–2789.
7. Yin, Z., Luo, B., Hong, W.. Separable and error-free reversible data hiding in encrypted image with high payload. *The Scientific World Journal* 2014;**2014**.