

Medical Image Encryption by Using Modification of SomdipDey Advanced Encryption Image Technique

Al Farissi
Informatics Engineering
Sriwijaya University
Palembang, Indonesia
alfarissi.ilkom@gmail.com

AgungWahyuNugroho
Informatics Engineering
Sriwijaya University
Palembang, Indonesia
agungnugrohoTM@gmail.com

MegahMulya
Informatics Engineering
Sriwijaya University
Palembang, Indonesia
megahmulya@yahoo.com

Abstract—The rapid growth of technology led the security of data becomes a very important issue, in particular data on medical field. Therefore the security of data need to be considered. This research will focus on the security of medical image. The appropriate technologies to increase the security of medical image is the image encryption. This research, applied a technique that can encrypt a medical image, it is SompdipDey Advanced Encryption Image Technique. This technique has three phases, namely Bits Rotation and Reversal, Extended Hill Cipher and Modified MSA Randomization. This research was also conducted on a modification of the stage Extended Hill Cipher that produces a better result so that the security of medical data will be increased.

Keywords— Medical Image, Image Encryption, Modification, SD-AEI, Hill Cipher;

I. INTRODUCTION

With growing technology, data security becomes a very important issue. In an article written by the New England Journal of Medicine states that, often occurs theft of data in medical section [5]. Therefore, the security of data in the medical section requires special attention. The image is part of the medical data that will need security. Image is a visual representation of something that contains information. It contrasts with the text, the image has own its uniqueness because in an image can have a lot of information. The images in the medical section are very secret images and not everyone should know about it. For example, x ray images of brain cancer. Therefore, an application that can encrypt with strong technique is needed. So that images are safe while in storage.

Referring to the problems described above, the main objective of this research is to improve security of image in the medical section. Encryption for digital image is the best approach used to resolve this problem [4]. By using encryption, confidentiality of medical digital images will be protected when stored in storage. In this research, the techniques that may be appropriate to use is SompdipDey Advanced Encryption Image Technique [2] It is a technique

developed by SompdipDey by combining the three methods namely Bit rotation and reversal, Extended Hill cipher and Modified MSA Randomization [2]. But after doing research this technique has the disadvantage, namely if the key used when the decryption is almost the same as the original key, then the original image is almost visible so that the technique is modified. The modifications that have been done produces better results and resolve problems that occur in the method before modified.

The technique, SompdipDey Advanced Encryption Image Technique, which is used to encrypt the images follows the following algorithm:

Stage-1: Bits rotation and reversal method based on password

Stage-2: The Extended Hill Cipher technique for Image Encryption.(Modification)

Stage-3: Modified MSA Randomization

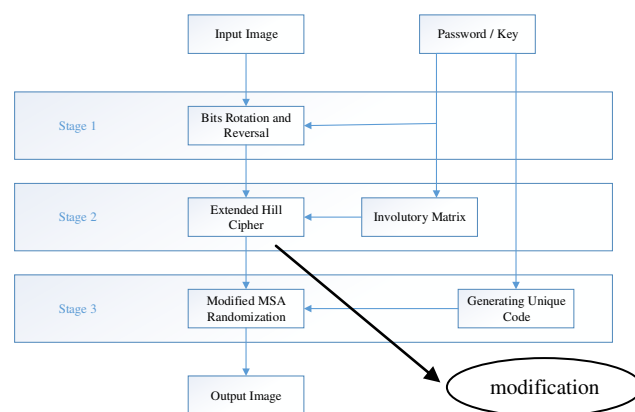


Fig 1. Block Diagram of SompdipDey Advanced Encryption Image Technique

II. ALGORITHM OF SOMPDIP DEY ADVANCED ENCRYPTION IMAGE TECHNIQUE

1) BITS ROTATION AND REVERSAL

Bits Rotation and Reversal process is the first stage of the technique used in this study. At this stage, the value of each

pixel is 24 bits divided into three colours. Key length used for rotation and reversal. Each 8-bit color that has passed this step must unite again to the value of 24-bit pixels then change that occur for the value of each pixel of the input image, because bits rotation and reversal generate an encrypted image.

Example:

11000101 ← Example of the value of a color
 "Sandi" ← Example of key with length 5 characters

LR = 5 mod 7
 LR = 5
 = 11000101
 = 10111000
 = 00011101 ← Bit rotation and inversion results

2) EXTENDED HILL CIPHER

Extended Hill Cipher process is the second stage of the technique used in this research. At this stage there are three steps that will be passed are:

Step 1: An Involutory Matrix 4x4 is formed by using a key[1][3] To generate an Involutory Matrix, minimum length of alphanumeric password should be four.

Step 2 (Modification): Value of each row of pixels is converted into binary numbers. Binary rearranged in reverse order. After that, the binary number is converted again into a decimal number. Therefore, the value of each pixel will change because the value of bits per pixel has been reversed. And it is also done with the columns of the input image.

Example:

TABLE I
EXAMPLE OF PIXELS IN DECIMAL FORM

11	12	13	14
21	22	23	24
31	32	33	34
41	42	43	44

TABLE II
TABLE OF PIXELS THAT HAVE CHANGED IN BINARY FORM

001011	001100	001101	001110
010101	010110	010111	011000
011111	100000	100001	100010
101001	101010	101011	101100

TABLE III
TABLE OF PIXELS THAT HAVE BEEN REVERSE BY ROW

011100	101100	001100	110100
000110	111010	011010	101010
010001	100001	000001	111110
001101	110101	010101	100101

TABLE IV
TABLE OF PIXELS THAT HAVE BEEN RETURN IN DECIMAL FORM

28	44	12	52
6	58	26	42
17	33	1	62
13	53	21	37

TABLE V
TABLE OF PIXEL BINARY WITH THE NEW VALUE

011100	101100	001100	110100
000110	111010	011010	101010
010001	100001	000001	111110
001101	110101	010101	100101

TABLE VI
TABLE OF PIXELS THAT HAVE BEEN REVERSED BY THE COLUMN

101100	101011	101010	101001
100010	100001	100000	011111
011000	010111	010110	010101
001110	001101	001100	001011

TABLE VII
TABLE OF PIXELS FOR FINAL DECIMAL

44	43	42	41
34	33	32	31
24	23	22	21
14	13	12	11

In the second step of the Extended Hill Cipher stage can be analysed that when the number of bits carried rearrangements in reverse on every row, then the resulting value will be changed completely from the original value and when the number of bits carried rearrangements in reverse on each column of pixels, then the value will be returned to original, only pixel values will switch positions. So from the analysis conducted when rearrangements of bits in reverse only done on row then it will produce better images encrypted and in this research will only apply a reversal on the row.

Step 3: The results of step 2 the image is processed again with Involutory Matrix[1][3] that was created in step 1 to get the final result of the Extended Hill Cipher method.

3) MODIFIED MSA RANDOMIZATION

The Modified MSA Randomization process is the last process in the Sompdip Day Advanced Encryption Image Technique. At this stage, the whole image is broken down into a number of blocks of the image and then randomization technique is applied to each block of the image file. After randomization method is complete, each block is written in the output file as a final encrypted image.

Modified MSA Randomization algorithm involves the following steps:

Step-1: Function Cycling()

Step-2: Function Upshift()

Step-3: Function Rightshift()

Step-4: Function Left Diagonal Randomization()

Step-5: Function Cycling() for “code” number of times

Step-6: Function Downshift()

Step-7: Function Leftshift()

Step-8: Function Right Diagonal Randomization()

In Cycling, upshift, Rightshift, and Left Diagonal Randomization functions are repeated n times depending on the value of the unique code generated from the key. To find out how to generate a unique code will be explained below

4) GENERATING UNIQUE CODE

This step is needed to generate a unique code from the key (symmetric key) that is used in the Modified MSA Randomization stage to encrypt and decrypt the image file. The code generated from the key or key is case sensitive because to generate a unique code the steps are manipulating every bit key so that if there is the slightest change then the result would be different.

Forexample, if $P_1 P_2 P_3 \dots P_{len}$ is the character of the key where key length starting from 1, 2, 3, 4, ..., len . First step is to multiply 2^{by_i} where i is the position of the character key. All the characters in the key have been changed to an ASCII value. Do this step until all characters is complete. And then add all of the multiplication results into a number. After added, the value is separated into each character and each character value is added again to become the new number.

Example of key: AbC

$P_1 = A = 65$

$P_2 = b = 98$

$P_3 = C = 67$

$N = 65 * 2^{(1)} + 98 * 2^{(2)} + 67 * 2^{(3)} = 1058$

Unique Code = $1 + 0 + 5 + 8 = 14$

III. RESULTS AND DISCUSSIONS

After testing in encryption and decryption process by using image with any resolution. And also after testing on the technique that has been modified so that the results obtained are quite different from the techniques prior to modification. Including the simulation time that required technique which has been modified faster than techniques that have not been modified and when the decryption process on techniques that have not been modified using a key which is almost same as original key, the original image is almost visible while on a technique that has been modified is not visible at all. Further information about the results of the

above test will be described in the following table VIII which testing table of Image 1000 x 998 pixels.

TABLE VIII
TESTING TABLE OF IMAGE


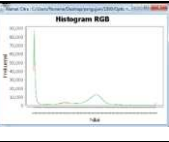

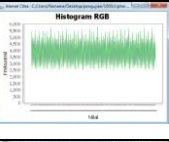


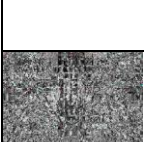

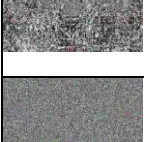



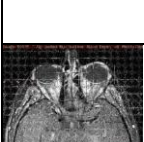

Image	Key	Histogram	Time Process	Information
	-		-	The original image that has not done the encryption process
	S a n d i		22.854 seconds	Encrypted image by using the key “sandi”
	S a n d i		16.414 seconds	Encrypted image from the techniques that have been modified using the key “sandi”
	1 2 3 4 5		21.276 seconds	Image of decryption result with any key namedly “12345”
	1 2 3 4 5		15.465 seconds	Image of decryption result from techniques that have been modified by using any key namedly “12345”
	S a n d		21.477 seconds	Image of decryption result by using a key that is almost the same as the real key namedly “sand”
	S a n d		15.642 seconds	Image of decryption result from the techniques that have been modified by using a key that is almost the same as the real key namedly “sand”

TABLE IX
ENCRYPTIONQUALITYTESTING.

Resolution (pixel)	MDF		CCF		IDF	
	Before Modification	After Modification	Before Modification	After Modification	Before Modification	After Modification
70 x 60	2938	3224	0.575694	0.528766	4200	4200
100 x 100	11708	11530	0.241948	0.185410	10000	10000
300 x 285	50759	57069	0.750709	0.685236	85500	85500
500 x 410	127352	124634	0.796444	0.809360	205000	205000
700 x 689	343433	309926	0.690679	0.729688	482300	482300
1000 x 998	812387	810066	0.468453	0.475810	998000	998000
1300 x 1082	825495	618225	0.897939	0.929919	1406600	1406600
1500 x 1323	1423795	1167837	0.730984	0.817644	1984500	1984500
1800 x 1700	2571202	2295724	0.563651	0.652941	3060000	3060000
2000 x 1800	1628395	1523622	0.750589	0.758846	3600000	3600000

In this study also tested the quality of the image encryption by using The Maximum Deviation Measuring Factor (MDF), The Correlation Coefficient Measuring Factor (CCF) and The Irregular Deviation Measuring Factor (IDF)[5]. At the MDF technique if the results is large then the quality encryption is better, at the CCF technique if the result is close to zero then the quality encryption is better, while in the IDF technique if the results is small then the quality encryption is better.

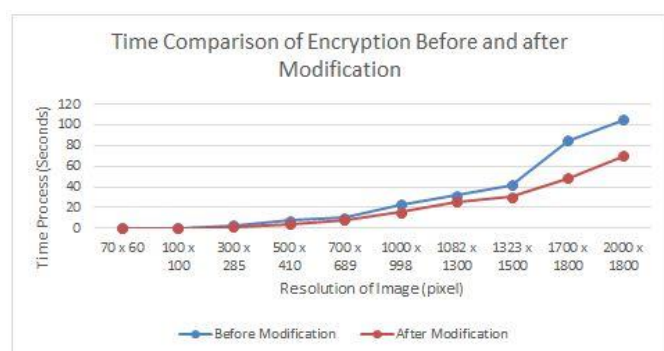


Fig. 2 Comparison Chart of Encryption Time Before and After Modification

IV. COMPARISON WITH OTHER ENCRYPTION TECHNIQUES

The technique that have not been modified namely SompdipDey Advanced Encryption Image Technique proposed in this paper, is compared with other encryption techniques like SompdipDey Encryption Image (SD-EI)[6], MSA and TTJSA [7].

TABLE 4 shows the difference between SD-AEI encryption technique and other encryption techniques on the basis of time taken to encrypt/decrypt and the encryption processes were executed using “sandi” as password.

TABLE X
TIME TAKEN TO ENCRYPT/DECRYPT IN SECONDS (SECS)

Image Size	SompdipDe y Encryption image	SompdipDey Advanced Encryption Image Technique	MSA	TTJSA
512 B	2	2	1	2
1 KB	2	3	2	3

512 KB	4	5	3	4
1 MB	6	6	5	7

V. CONCLUSION

Here, based on the analysis, implementation and testing that has been done in this study, it can be concluded as follows:

1. After testing, a modified technique has several advantages including the time it takes to process faster, and when decryption process done on a technique that has not been modified using key almost the same with key that was used when encryption process then the original image almost looks while when done the technique has been modified original image is not visible at all.
2. When performing encryption or decryption process by using the exact same input data then the time required will not always be the same because it depends on the condition of the computer.
3. The larger the image resolution then comparison time between technique has been modified with original technique getting away as shown in Figure 2.
4. Security of medical digital images was increased by applying SompdipDey Advanced Encryption Image Technique but when applying SompdipDey Advanced Encryption Image Technique that has been modified medical digital image security would be more increased compared with techniques that have not been modified

REFERENCES

- [1] Bibhudendra. A., Panigrahy. S. K., Patra. S. K. and Panda. G., “Image Encryption Using Advanced Hill Cipher Algorithm”, International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009, pp. 663-667.
- [2] Dey, S., “SD-AEI: An advanced encryption technique for images,” Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on, 10-12 July 2012 2012a. 68-73.
- [3] Saroj K. P., Acharya. B. and Jena. D., “Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm”, 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.
- [4] Yicong, Z., Panetta, K. and Agaian, S., “A lossless encryption method for medical images using edge maps,” Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE, 3-6 Sept. 2009 2009. 3707-3710.
- [5] (2013) The NEJM website. [Online]. Available: <http://www.nejm.org/doi/full/10.1056/NEJMp1215258>
- [6] Dey, S., “SD-EI: A Cryptographic Technique To Encrypt Images”, Proceedings of “The International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec 2012)”, held at Kuala Lumpur, Malaysia, 2012, pp. 28-32.
- [7] Nath, A., Chatterjee, T., Das T., Nath J and Shayan Dey, “Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSA method: TTJSA algorithm”, Proceedings of “Information and Communication Technologies (WICT), 2011 “ held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.