Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security

Candra Irawan\textsuperscript{1}, De Rosal Ignatius Moses Setiadi\textsuperscript{1}, Eko Hari Rachmawanto\textsuperscript{1}, Christy Atika Sari\textsuperscript{1}, Mohamed Doheir\textsuperscript{2}

\textsuperscript{1} Department of Informatics Engineering, Dian Nuswantoro University, 207 Imam Bonjol Street, Semarang 50131, Indonesia
\textsuperscript{2} Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Abstract. The medical image is an image that needs to be protected because it is private and confidential. The more modern technology enables tele surgery, tele diagnosis, and others to demand safe and confidential medical images. This research proposes cryptography method in a medical image by using the combination algorithm of Arnold chaotic map (ACM) and Rivest Cipher 4 (RC4). ACM is a chaotic cryptographic technique superior to attack deferential attack and brute force. The way chaotic cryptography works is to confuse the pixel location. While RC4 is a stream cipher technique that has resistance to statistical attacks and fasts in computing. The purpose of merging these two algorithms is to get stronger encryption techniques, have good performance, and can be computed quickly. Based on the experimental results proved that the use of a combination of these two algorithms can produce satisfactory quality encryption. This is evidenced by several measuring tools such as SSIM, Correlation Coefficient, Entropy, NPCR, UACI, and histogram analysis. Computation time required is also relatively very fast ie less than one second, where computational time is calculated by tic toc function.

1. Introduction
The medical image is one of the important images that need to be protected because it is private and confidential. Current technological developments have enabled modern things such as telemedicine, telediagnosis, telesurgery and others which require the delivery of medical images. Commonly delivery image uses the internet network is not necessarily safe. At the time of delivery of medical images, medical images must be guaranteed the availability, safety, and confidentiality [1] [2] [3]. Cryptography is a very important coding technique to secure data in communication systems [4] [5] [6] [7], so it can be used as a solution to secure the medical image when sent. Cryptography on images is often called visual cryptography, this is because the results of image encoding can significantly change the meaning of the image visually [4] [8].

The popular cryptographic techniques on the image are the confused pixel location and pixel value substitution [4] [9]. Chaos technique is the most popular to perform confused pixel locations. This technique is very sensitive to the initial conditions, and has ergodicity and boundedness properties, so that this technique can meet certain security conditions [10] [11], this technique is also sensitive to small changes in the input parameter and has a high level of security against brute-force attacks and attack deferential [12]. Some commonly used chaos algorithms are Arnold, Henon, and Logistic map. One technique of pixel value substitution is a stream cipher algorithm with Rivest Cipher 4 (RC4). RC4 is an encryption technique that uses symmetric keys. The symmetric key is used to generate 256-bit key stream keys with permutations. The permutation result is then randomized with pseudo-random
function and XOR operator to generate ciphertext [13] [14]. The advantages of the RC4 algorithm is a fast and powerful computation time against statistical attacks. RC4 can also change the image pixel value so that the pixel value distribution on the cipher image histogram becomes relatively uniform. The difference between chaos and stream cipher techniques in digital images is on the resulting encryption and resistance to different attack models. The chaos technique only performs pixel confused on imagery by key and iteration, while the stream cipher changes the pixel value of the image by key. Thus, the study aims to improve the security of medical images by combining both techniques with the Arnold and RC4 algorithms.

2. Related Research
In the study of Ismael et al. [15] the RC4 method is implemented to encrypt images. Then the results of the encryption are tested with several types of tests. The first test is histogram analysis, the result shows that the histogram distribution which is initially not uniform, changes to be relatively uniform from pixels that are worth 0 to 255. The second test is FIPS 140, which consists of four types of tests namely Poker, Run, Long Run and Monobit. FIPS 140 test is a standard test that is approved by NIST. From all tests carried out RC4 algorithm fulfilled and passed all the specified criteria, so it can be concluded that RC4 is an algorithm that is resistant to various attacks and has a high level of image randomization.

Another study conducted by Bhogal et al. [16] combined the Chaotic Map method with the AES method to encrypt medical images. In his research, input images in the form of DICOM images with 16 bits are used as plain images. Furthermore, the image is encrypted using the Chaotic map, the result of encryption is then expanded to 8 bits or grayscale with a width of twice the size of the plain image. Furthermore, AES encryption is performed on the expansion image to produce a cipher image. Based on cipher image testing the proposed method is superior to histogram and correlation tests when compared to the AES method only.

Naveenkumar et al. [11] proposed a technique for expansion and shrinkage in the chaotic map method. This is because the chaotic map technique only performs randomization on pixels, so the results of image encryption choose the same histogram. In his research, an input image is expanded from the size of m, n to m, 8 * n, so that images with a depth of 8 bits become images with 1 bit. Furthermore, the image is encrypted with the chaotic map. The results of the encryption are then depreciated to their original size (m, n). Based on testing this method is able to increase the entropy value and uniformity of the histogram.

From some of the above studies, it was found that a hypothetical chaotic map method is an encryption method that only performs sprinkling so that it needs to be upgraded with a substitution method. RC4 is a method that is resistant to various attacks, so combining RC4 and chaotic map methods will result in stronger encryption.

3. Research Method
This section consists of three stages, ie, encryption, decryption, and finally evaluation of the performance of the proposed method.

3.1. Encryption Method
The process of image encryption is done through two main stages, the first stage is encrypted with Arnold chaotic map (ACM) followed by RC4. Here are the detailed steps of the encryption process.

1. Perform a confused pixel value on the input image using the ACM algorithm, where the initial conditions and iteration parameters serve as the first secret key. The ACM formula is defined by (1) [17]. Save ACM encryption result on variable $E_i$.

$$\begin{pmatrix} X_{n+1} \\ Y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab + 1 \end{pmatrix} \begin{pmatrix} X_n \\ Y_n \end{pmatrix} \mod N$$

Where $X_n,Y_n = \{0,1,2,...,N\}$ is pixel coordinate of the original plain image

2. On the other hand, generate a key stream with a key input with a string type with permutations of 256 iterations, then save the result in an S-box. Use pseudocode (2) to complete this stage.
Input : RC4 key
Output : key stream (S-Box)
1. i=1;j=1; Sbox = 0:255;
2. while i<=256
3. j = 1 + mod(j + Sbox(i) + key(1 + mod(i, keylength)), 256);
4. swap(Sbox(i), Sbox(j));
5. i++; 

3. Perform pseudo-random on S-Box then save on pKey variable with pseudo code (3) below.
Input : key stream (S-Box)
Output : pKey stream (pseudo-key)
1. i=1;j=1; n = number_of_pixel_Image;
2. while k<=n
3. i = 1 + mod(i + 1, 256);
4. j = 1 + mod(j + Sbox(i), 256);
5. swap(Sbox(i), Sbox(j))
6. pKey = 1 + mod(Sbox(i) + Sbox(j), 256);

4. Perform bitwise XOR on S-Box (pKey) and \( E_i \) with iteration to get encrypted image \( E2i \).

3.2. Decryption Method
Same with the process of encryption, decryption process also through two stages of decryption that is with RC4 and ACM. The difference is in the process of decryption algorithm RC4 done first. Here are detailed steps of the decryption process:
1. Generate key streams with the same key input as the encryption process using permutations of 256 iterations, then save the result in an S-box. Use pseudocode (2) to complete this stage.
2. Perform pseudo-random on S-Box using pseudo code (3), then save on pKey variable
3. Perform bitwise XOR on S-Box (pKey) and \( E2i \) using looping so get decrypted image \( D_i \).
4. Perform ACM on image decryption \( D_i \) with formula (1) according to the number of iter when performing encryption, so as to get decryption image \( D2i \).

3.3. Evaluation and Measurement
SSIM is an extension of the Structural Similarity Index, the SSIM value obtained by comparing the original image and the encrypted image based on luminance, contrast and its structure [4]. SSIM can be calculated by the formula(4).

\[
SSIM \ (p,e) = \frac{(2\mu_p\mu_e + c_1)(2\sigma_{pe} + c_2)}{\mu_p^2 + \mu_e^2 + c_1(\sigma_p^2 + \sigma_e^2 + c_2)} \ 
\]

Where \( p \) is a plain image ; \( e \) is an encrypted image; \( \mu_p \) and \( \mu_e \) is mean of the \( p \) and \( e \) images; \( \sigma_{pe} \) is the image covariance \( p \) against \( e \); \( \sigma_p^2 \) is a variant of the plain image; \( \sigma_e^2 \) is a variant of an encrypted image; \( c_1 = (k_1D)^2 \) and \( c_2 = (k_2D)^2 \); \( D \) is a dynamic range of the image \( (2^b - 1) \) with the default value \( k_1 = 0.01 \) and \( k_2 = 0.03 \). Smaller SSIM values indicate that an encryption is secure, and vice versa. Whereas Entropy is used to calculate the probability of a decrypted image opportunity, which can be calculated by the formula (5). The good and safe entropy value of the attack is close to eight [4] [7] [18].

\[
E = - \sum_{i=0}^{255} p(i) \log_2(p(i)) \ 
\]

Where \( E \) is Entropy; \( p(i) \) is chance of probability. NPCR stands for the number of pixel change rate while UACI stands for unified average changing intensity. These two measuring instruments serve to analyze the strength of the proposed method of differential attack. If the encryption algorithm has a
diffusion or confusion stage it should not be easily solved by differential attack [11] [12] [19]. Formula (6) is used to calculate NPCR, whereas UACI can be calculated by the formula (7).

\[
NPCR = \frac{1}{M \times N} \sum_{x=0}^{M} \sum_{y=0}^{N} D(x, y) \times 100% , \tag{6}
\]

\[
D(x, y) = \begin{cases} 
0, & I_1(x, y) = I_2(x, y) \\
1, & I_1(x, y) \neq I_2(x, y)
\end{cases}
\]

\[
UACI = \frac{1}{M \times N} \sum_{x=0}^{M} \sum_{y=0}^{N} \frac{|I_1(x, y) - I_2(x, y)|}{255} \times 100% \tag{7}
\]

Where \(I_1\) and \(I_2\) are two images with same size \(M\) and \(N\), \(x\) and \(y\) is coordinate pixel location based on \(M\) and \(N\). The greater the NPCR value indicates that the better the encryption quality, while the smaller UACI value signifies better encryption results. At the decryption stage also measured with the correlation coefficient, value 1 indicates that the image decryption can be done perfectly [20] [21].

Formula (8) is used to calculate the correlation coefficient value.

\[
cc = \frac{\sum_m \sum_n (I_1 - \bar{I}_1)(I_2 - \bar{I}_2)}{\sqrt{(\sum_m \sum_n (I_1 - \bar{I}_1)^2)(\sum_m \sum_n (I_2 - \bar{I}_2)^2)}} \tag{8}
\]

Histogram analysis is also used to measure image quality of encryption and decryption results, if the histogram result is uniformly it means the encryption results are better. The computational speed of the proposed method on encryption and decryption methods is also measured by the tic toc function in Matlab.

4. Results and Analysis

At this stage, first collected a standard medical image downloaded from the MedPix website page [22]. The image file name and image size are also unchanged, as well as the image extension in accordance with the original format of MedPix is a JPEG file. Furthermore, the medical image is done encryption process, decryption and performance measurement. Figure 1 shows the sample images used in this study. In accordance with the proposed method of encryption process using a combination of two methods, where iterated 10 times on the ACM method, while the RC4 key is "udinus". Table 1 shows the image of encryption and histogram, while Table 2 shows the values of SSIM, Entropy, NPCR, UACI and Time Taken. Based on table 1, it is visually apparent that the encryption results of the proposed method completely change the shape of the image. The image of the encryption has no meaning, nor is the histogram before and after the encryption a significant difference. The pixel distribution value of the histogram is also well distributed, only in the black color (close to 0) and the white color (close to 255) has a relatively lower distribution, but in whole the distribution of pixel values can be uniform. Table 2 also suggests that very small SSIM values, almost perfect entropy values, and highly satisfactory NPCR and UACI values. Computation time required is also very fast, ie less than one second.

Decryption method is tested on the receiver side. Figure 2 shows the image decryption, while table 3 contains the result of Correlation Coefficient value and time needed for decryption. Because the proposed method uses a symmetric key, the key used in the decryption process is the same as the encryption process. Based on Figure 1 visually it appears that medical images can be perfectly decrypted, the decryption image histogram is also exactly the same as the original image. Table 3 also strengthens visual observation results, because based on mathematical calculations, the value of the correlation coefficient of the decryption method using the proposed method gets perfect value, that is 1. Perfect decryption is very important in medical images, because if the process of decryption changes the image then it can make the meaning of the image changed. Medical image changes are very dangerous if they occur, as they may affect a doctor's diagnosis.

Table 4 proves that the proposed method is better than the ACM or RC4 algorithm. The SSIM, Entropy, and NPCR values of medical image encryption appear superior to those of the other two
methods. This proves that the proposed method can perform better encryption. It's just that based on the UACI value, the ACM algorithm looks superior, but based on table 5, it appears that the histogram of the ACM method is exactly the same as the original image histogram. While RC4 has little advantage in spreading pixel values, pixel values around 0 and around 255 appear to be relatively more uniform compared to the proposed method as shown in Table 5.

Table 1. Encryption and Histogram Result from Proposed Encryption Method

| Original Image | Original Histogram | Encryption Result | Encryption Histogram Result |
|----------------|-------------------|-------------------|-----------------------------|
| synpic1007.jpg | ![Histogram](image) | ![Encryption Result](image) | ![Encryption Histogram](image) |
| synpic30200.jpg | ![Histogram](image) | ![Encryption Result](image) | ![Encryption Histogram](image) |
| synpic38476.jpg | ![Histogram](image) | ![Encryption Result](image) | ![Encryption Histogram](image) |
| synpic40237.jpg | ![Histogram](image) | ![Encryption Result](image) | ![Encryption Histogram](image) |

Table 2. The Value of SSIM, Entropy, NPCR, UACI and Time Taken Measurement Result from Proposed Encryption Method

| Image         | SSIM  | Entropy | NPCR     | UACI   | Time Taken (in a second) |
|---------------|-------|---------|----------|--------|--------------------------|
| synpic1007.jpg| 0.0096| 7.9951  | 0.996389 | 0.308210| 0.70557                  |
| synpic30200.jpg| 0.0055| 7.9946  | 0.996605 | 0.395958| 0.70615                  |
| synpic38476.jpg| 0.0057| 7.9952  | 0.996018 | 0.381952| 0.70656                  |
| synpic40237.jpg| 0.0069| 7.9943  | 0.995309 | 0.352458| 0.69726                  |
Table 3. The Value of Correlation Coefficient and Time Taken Measurement Result from Proposed Decryption Method

| Image         | Correlation Coefficient | Time Taken (in a second) |
|---------------|-------------------------|--------------------------|
| synpic1007.jpg| 1.0000                  | 0.70942                  |
| synpic30200.jpg| 1.0000                   | 0.71053                  |
| synpic38476.jpg| 1.0000                   | 0.77063                  |
| synpic40237.jpg| 1.0000                   | 0.77251                  |

Table 4. Comparative Encryption Result based on Value of SSIM, Entropy, NPCR, and UACI

| Image         | Method    | SSIM     | Entropy  | NPCR     | UACI     |
|---------------|-----------|----------|----------|----------|----------|
| synpic1007.jpg| ACM Only  | 0.0155   | 7.1624   | 0.983858 | **0.260081** |
|               | RC4 Only  | 0.0100   | 7.9940   | 0.996049 | 0.307243  |
|               | Proposed  | **0.0096**| **7.9951**| **0.996389** | 0.308210  |
| synpic30200.jpg| ACM Only  | 0.0031   | 6.5431   | 0.944475 | 0.418033  |
|               | RC4 Only  | 0.0089   | **7.9951**| 0.995771 | 0.308039  |
|               | Proposed  | 0.0055   | 7.9946   | **0.996605** | 0.395958  |
| synpic38476.jpg| ACM Only  | 0.0105   | 6.3666   | 0.962531 | **0.243635** |
|               | RC4 Only  | 0.0112   | 7.9950   | 0.995278 | 0.306650  |
|               | Proposed  | **0.0057**| **7.9952**| **0.996018** | 0.381952  |
| synpic40237.jpg| ACM Only  | 0.0106   | 6.0211   | 0.946790 | **0.268333** |
|               | RC4 Only  | 0.0099   | 7.9938   | **0.996296** | 0.308010  |
|               | Proposed  | **0.0069**| **7.9943**| 0.995309 | 0.352458  |
Table 5. Comparative Encryption Result based on Histogram

| Image Name         | ACM Only | RC4 Only | Proposed |
|--------------------|----------|----------|----------|
| synpic1007.jpg     | ![Image] | ![Image] | ![Image] |
| synpic30200.jpg    | ![Image] | ![Image] | ![Image] |
| synpic38476.jpg    | ![Image] | ![Image] | ![Image] |
| synpic40237.jpg    | ![Image] | ![Image] | ![Image] |

5. Conclusion
This research combines confused and stream cipher methods in medical images. Based on the theory of each method has their respective advantages, then by combining the two methods obtained stronger encryption results. Based on the results of testing the proposed method also proved superior compared with other methods. Of the five kinds of measuring instruments, namely SSIM, Entropy, NPCR, UACI and histogram analysis. SSIM, Entropy and NPCR values appear superior to other methods. So it can be concluded that the proposed method has better performance. The proposed method can also do the decryption perfectly; it is very important that no missing medical image information. The computation time required is also relatively fast where the required time during encryption and decryption is less than one second each. In the next study, this method can be developed again to increase the value of UACI and the distribution of histogram values more uniform.

6. References
[1] Boulimi, D., Coatrieux, G., Cozic, M. & Roux, C., 2012. A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images, IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 5, pp. 891 - 899.
[2] Shareef, M. P., V, D. T., Abraham, N., Babu, T. & KV, R. 2014. Encryption-Enhanced Reversible Watermarking for Medical Images via Prediction and RC4 Encryption, in International Conference on Communication and Signal Processing, Melmaruvathur.

[3] Boussif, M., Aloui, N. & Cherif, A. 2017. New Watermarking/Encryption Method for Medical Images Full Protection in m-Health, International Journal of Electrical and Computer Engineering, vol. 7, no. 6, pp. 3385-3394.

[4] Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., Susanto, A. & Doheir, M., 2018. A Comparative Study of Image Cryptographic Method, in International Conference on Information Technology, Computer and Electrical Engineering, Semarang.

[5] Najih, M., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., Astuti, S. 2017. An improved secure image hiding technique using PN-sequence based on DCT-OTP, in International Conference on Informatics and Computational Sciences, Semarang.

[6] Rachmawanto, E. H., Amin, R. S., Setiadi, D. R. I. M. & Sari, C. A. 2017. A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size, in International Seminar on Application for Technology of Information and Communication, Semarang.

[7] Setyono, A., Setiadi, D. R. I. M. & Muljono, 2018. Dual Encryption Techniques for Secure Image Transmission, Journal of Telecommunication, Electronic and Computer Engineering. vol. 10, no 3-2, pp. 41-46.

[8] Ardy, R. D., Indriani, O. R., Sari, C. A., Setiadi, D. R. I. M. & Rachmawanto, E. H. 2017. Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5), in International Conference on Smart Cities, Automation & Intelligent Computing Systems, Yogyakarta.

[9] Rani, M. & Kumar, S. 2015. A Novel and Efficient Approach to Encrypt Images using Chaotic Logistic Map and Stream Cipher, in International Conference on Green Computing and Internet of Things, Noida.

[10] Abdullah, H. N. & Abdullah, H. A. 2017. Image Encryption Using Hybrid Chaotic Map, in International Conference on Current Research in Computer Science and Information Technology, Slemani.

[11] Naveenkumar, N. K., Panduranga, H. T. & Kiran, 2014. Chaos Based Image Encryption using Expand-Shrink Concept, International Journal of Informatics and Communication Technology, vol. 3, no. 2, pp. 103-112.

[12] Sethi, N. & Vijay, S. 2014. A New Cryptographic Strategy for Digital Images, International Journal of Electrical and Computer Engineering, vol. 4, no. 3, pp. 456-462.

[13] Bhowmick, A., Sinha, N., Arjunan, R. V. & Kishore, B., 2017. Permutation-Substitution Architecture Based Image Encryption Algorithm Using Middle Square and RC4 PRNG, in International Conference on Inventive Systems and Control, Coimbatore.

[14] Suresh, V. & Saraswathy, C. 2013. Separable Reversible Data Hiding Using RC4 Algorithm, in International Conference on Pattern Recognition, Informatics and Mobile Engineering, Salem.

[15] Ismael, R. S., Youail R. S. & Wahhab, S. 2014. Image Encryption by Using RC4 Algorithm, European Academic Research Journal, vol. 2, no. 4, pp. 5833-5839.

[16] Bhogal, R. S., Li, B., Gale, A. & Chen, Y. 2018. Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard, I.J. Information Technology and Computer Science, vol. 10, no. 8, pp. 1-10.

[17] Kusuma, E. J., Sari, C. A., Rachmawanto E. H. & Setiadi, D. R. I. M. 2018. A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography, Journal of ICT Research and Applications, vol. 12, no. 2, pp. 103-122.

[18] Putrie, V. M., Sari, C. A., Setiadi, D. R. I. M. & Rachmawanto, E. H. 2018. Super Encryption using Transposition-Hill Cipher for Digital Color Image, in International Seminar on Research of Information Technology and Intelligent Systems, Yogyakarta.

[19] Ismail, S. M., Said, L. A., Rezk, A. A., Radwan, A. G., Madian, A. H., Abu-ElYazeed, M. F. & Soliman, A. M. 2017. Image Encryption based on Double-Humped and Delayed Logistic Maps for biomedical applications, in International Conference on Modern Circuits and Systems Technologies, Thessaloniki.
[20] Irawan, C., Setiadi, D. R. I. M., Sari, C. A. & Rachmawanto, E. H. 2017. *Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption*, in International Conference on Informatics and Computational Sciences, 2017.

[21] Kusuma, E. J., Indriani, O. R., Sari, C. A., Rachmawanto, E. H. & Setiadi, D. R. I. M. 2017. *An Imperceptible LSB image Hiding on Edge Region using DES Encryption*, in International Conference on Innovative and Creative Information Technology, Salatiga.

[22] MedPix, "MedPix," Lister Hill National Center for Biomedical Communications, [Online]. Available: https://medpix.nlm.nih.gov/home. [Accessed April 2018].