Concordia University
Engineering and
Computer Science

Novel Image Compression-encryption hybrid algorithm based on a key-controlled measurement matrix in compressive sensing

Report Submitted by
Mofehintoluwa Ogunrinde (40019040)
Shawn Simpson (40058561)
Mehakpreet Singh (40057337)

Date: (21/12/2018)

Table of Contents

Table of Contents

1. Introduction

The security of images has become a high priority in the multimedia and technological world of information. The value of the image is dependent on the information of which it holds, techniques of image encryption have been developed and proposed to adhere to the protection of images. The newly sampling-reconstruction technique compressive sensing has been used along with other encryption methods to enhance the security of an image. This technique completes sampling and compressing simultaneously. Previous research has proven that the technique highlighting it's high performance. Compressive sensing based encryption has been found to be computationally secure and robust; the inherent multidimensional projection perturbation feature of the technique makes privacy breaching difficult. However, existing compressive based encryption algorithms adopted the whole measurement matrix as the key this results in a key which is too large in size to allocate or distribute and strenuous to memorize. In the previous scheme performing the compression and the encryption simultaneously was infeasible, leading to inefficiency. To overcome these challenges these challenges a hybrid compression technique where the measurement matrix is controlled by keys and constructed as a circulant matrix was developed. The original image is divided into 4 blocks to compress and encrypt then the 4 compressed and encrypted blocks are scrambled by random pixel exchanging with the random matrices.

1.1 Problem statement:

The problem with the image encryption algorithms presently in use is that the size of the key to encrypt is very large (usually about the size of the image). With this image encryption algorithm, the size of the key is reduced dramatically i.e. We only use two keys of 2 bits each.

This algorithm also adds image compression as an extra feature on top of encryption which makes this algorithm even better than other techniques. So, The picture sent over the network is even more secure and yet uses lesser network bandwidth.

2. Methodology

The process of encryption and decryption is divided into 3 stages each. As illustrated in the diagram below:

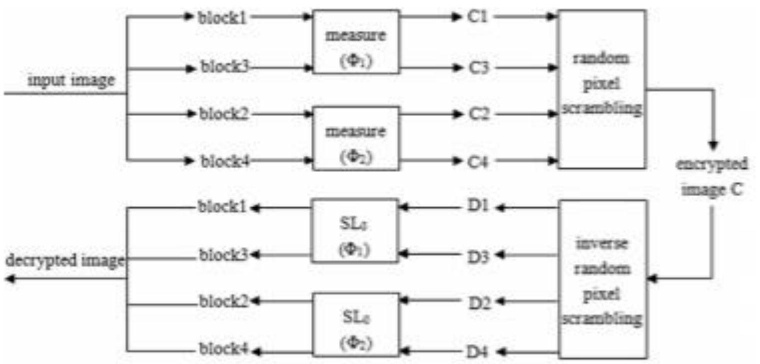


Fig 1. The process of proposed encryption algorithm in phases by Nanrun Zhou et al.

Stage1: At the first stage the input image of size 256x256 was divided into four (4) blocks, each block of size 128x128 (N/2 x N/2).

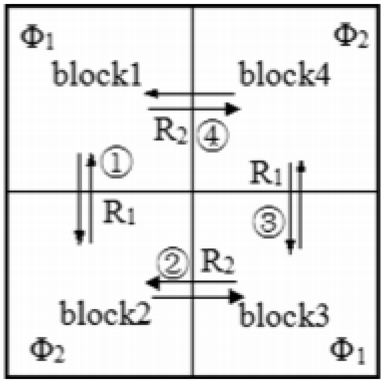


Fig. 2 method of dividing image and the order of random pixel scrambling by Nanrun Zhou et al.

Stage 2: A measurement matrix is constructed as a circulant matrix. The row vector of the matrix is controlled by a logistic map.

At this stage we considered:
The sender has two keys x1 and x2. And followed the steps below to measure the images.

Step 1:

The sender uses these two keys to create two **logistic maps**.
Logistic maps are created by putting the keys into the formula:

$$Xn+1 = \omega * Xn * (1-Xn)$$

We use this formula to get two logistic maps of size N/2.

Step 2:

The two logistic maps of size N/2 serves as the first rows of two measurement matrices. The following ((N/2)-1) rows are computed by applying the right circular shift to its preceding row.

Step 3:

Now we have two measurement matrices m1 and m2.
We measure block 1 and 3 with m1 and block 2 and 4 with m2.

After measuring we get the compressed version of the original photo that can be represented with much fewer attributes than the original.

Stage 3: Random pixel scrambling

The random pixel exchange process is applied to the grouped blocked of the image, I1, and I2 as illustrated in Fig.1 below.
M, N are the indices of the matrices.
R is the random matrix and its elements are limited to the interval [0,1]

Therefore, the pixels from each block from the left(I1) is exchanged with the pixels from the right side(I2).
This exchange gives a new value to the I1 and I2.

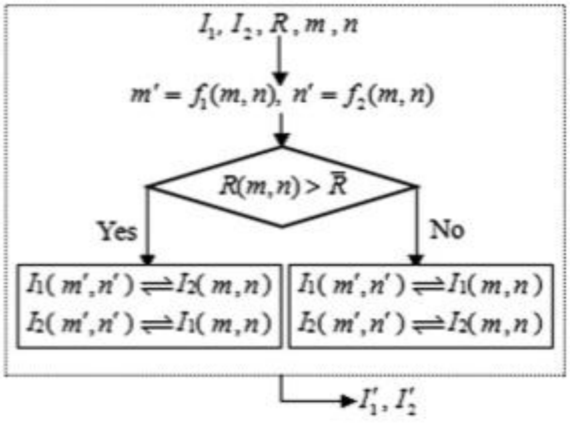

I_1, I_2, R, m, n
$m' = f_1(m,n), n' = f_2(m,n)$
$R(m,n) > \bar{R}$
Yes
No
$I_1(m',n') \rightleftharpoons I_2(m,n)$
$I_2(m',n') \rightleftharpoons I_1(m,n)$
$I_1(m',n') \rightleftharpoons I_1(m,n)$
$I_2(m',n') \rightleftharpoons I_2(m,n)$
I_1', I_2'

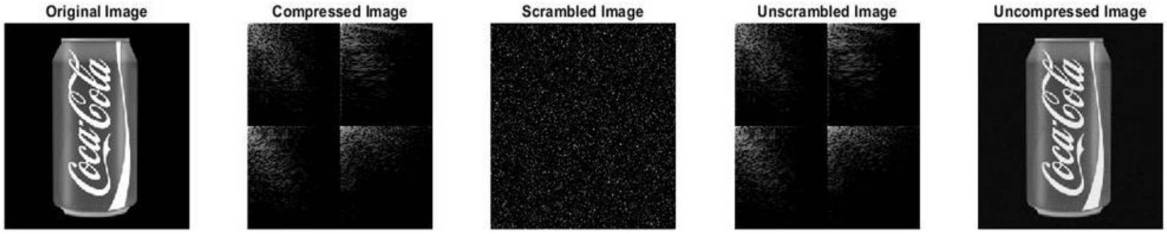
Fig. 3 Random Pixel Exchanging

Meanwhile, as illustrated in Fig 2, Since both the ranges of R1 and R2 are [0, 1], the ranges of measurement matrices Φ1 and Φ2 are [0, λ], and the sizes of measurement matrices are the same as R1 and R2, set R1 =Φ1/λ, R2 = Φ2/λ.

The decryption and decompression process were simply an inverse of the encryption and compression process as illustrated by Fig 1.

3. Experimental Results

Fig. 4: Snapshot of results of each stage with different images:



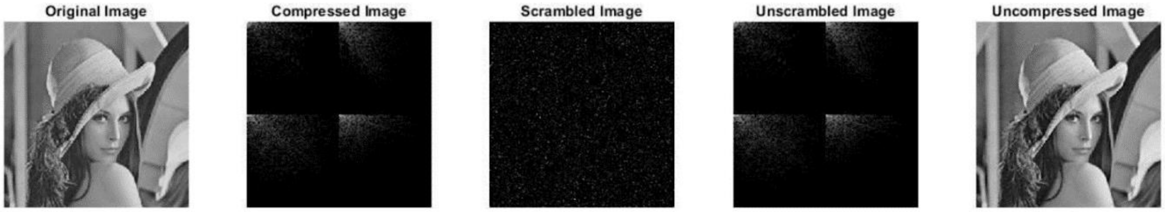
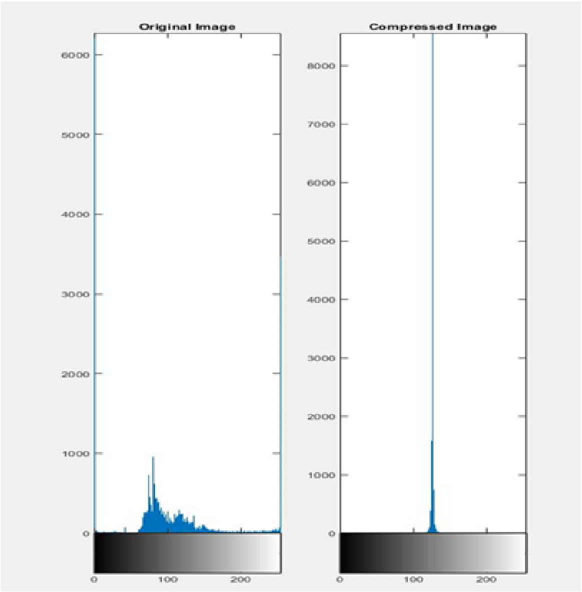


Fig 5: Histogram of Original vs Histogram of Encrypted and Compressed Image



4. Steganography

Compressive Sensing has been used to enhance security in Steganography where information is hidden within images and has proven to be very useful. The most well-known and commonly used image steganographic method is LSB Steganography in which the least significant bits (LSBs) of the cover image pixels are replaced with the secret information. LSB watermarking method with the hybrid compressive-encryption algorithm was combined.

Fig 6: Snapshots of a steganographic image at each stage.

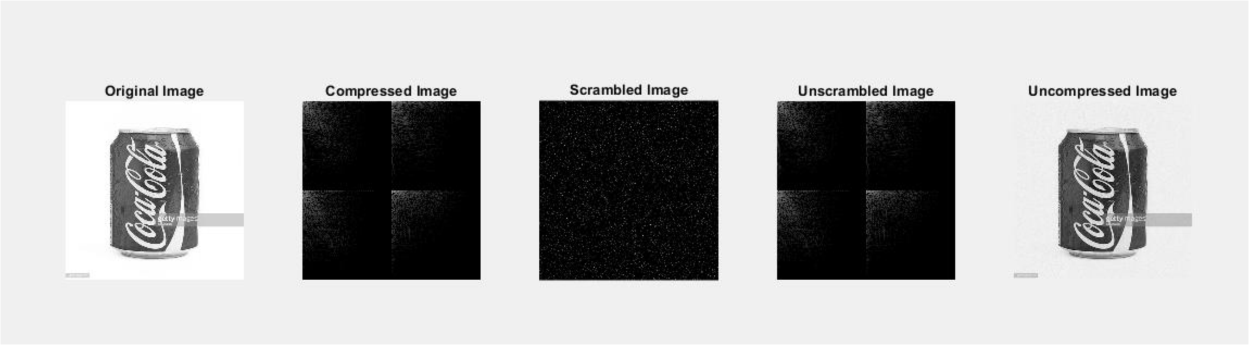


Fig 6: Snapshot of the hidden image and objective image in which it is hidden.

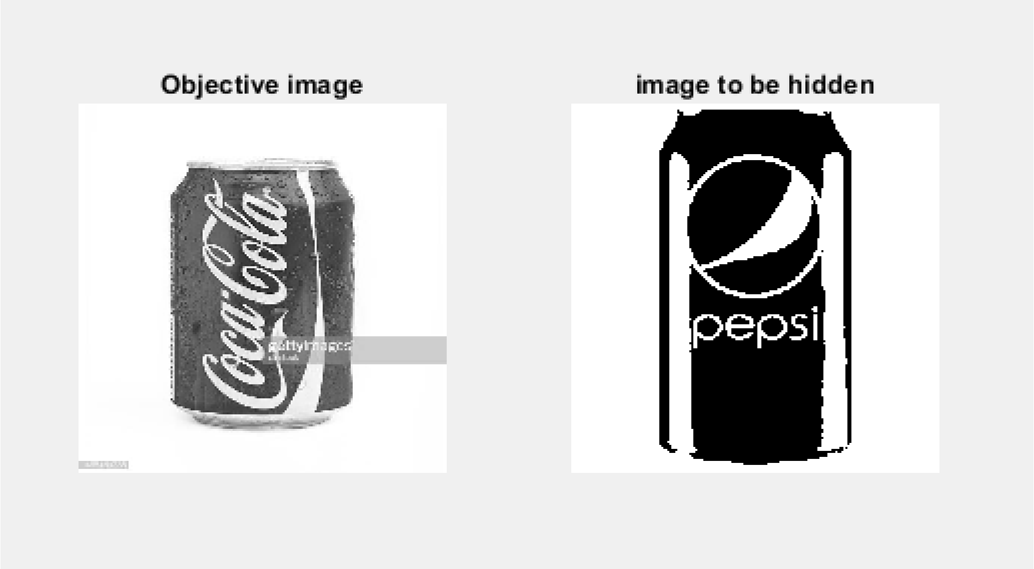
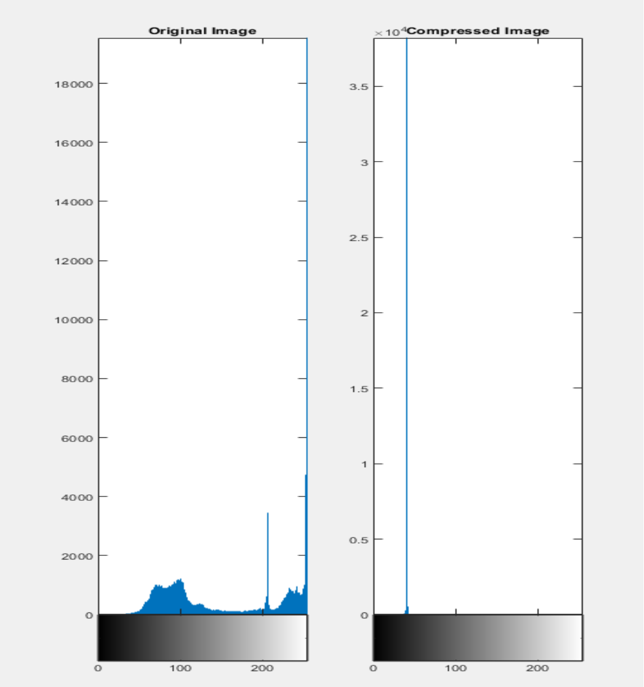


Fig 7: Histogram of Original Image with hidden information vs Histogram of Compressed Image with hidden information



5. Conclusion

This hybrid compression encryption algorithm based on compressive sensing and random pixel exchanging has proven overcome obstacles that have proven to be challenging for previous algorithms of its kind. The measurement key has been shortened significantly to just 2 bits in comparison to the M x N length keys which are used in other techniques. By shortening the key; distribution and memorization is now a more feasible task. The algorithm is also a more practical encryption technique by employing the circulant matrix to construct the measurement matrix of the compressive sensing and controlling the original row vector of the circulant matrix with a chaos logistic map; the encryption level is highly unassailable to threats. The algorithm enhances the security even further by random pixel exchanging and binding the random matrices with the measurement matrices. This report shows that this hybrid algorithm can offer high levels of security and compression results. High security in which this algorithm uses can be useful areas such as Steganography, where compressive sensing have been utilized and explored with. As shown in **figure 7**; combining compressive sensing with the least significant bit technique showed positive evidence of the ability and possible role this new hybrid compressive sensing-encryption algorithm can play. Further research is needed to compare this hybrid technique with previous techniques in Steganography; with it's an improvement at the encryption and security level along with its practicability only outstanding results can be expected.

6. References

1. Mohimani, H., Babaie-Zadeh, M., & Jutten, C. (2009). A Fast Approach for Overcomplete Sparse Decomposition Based on Smoothed Norm. IEEE Transactions on Signal Processing, 57(1), 289-301. doi:10.1109/tsp.2008.2007606
2. Zhou, N., Zhang, A., Zheng, F., & Gong, L. (2014). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Optics & Laser Technology, 62, 152-160. doi:10.1016/j.optlastec.2014.02.015
3. Chan, C., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition,37(3), 469-474. doi:10.1016/j.patcog.2003.08.007
4. Ulker, M., & Arslan, B. (2018). A novel secure model: Image steganography with logistic map and secret key. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). doi:10.1109/isdfs.2018.8355320
5. Zhang, B., Lei, Q., Wang, W., & Mu, J. (2013). Distributed video coding of secure compressed sensing. Security and Communication Networks,8(14), 2416-2419. doi:10.1002/sec.828
6. Sharma, N. K. (2017, September 25). LSB Watermarking: Simple code for 1 bit-LSB watermarking. Retrieved November 19, 2018, from https://www.mathworks.com/matlabcentral/fileexchange/64535-lsb-watermarking
   Source of the Code for Steganography.
   Chen W, Chen XD, Sheppard Colin JR. Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution. J Opt 2012;14:075402.
7. Chen W, Chen XD. Optical image encryption based on multiple-region plaintext and phase retrieval in three-dimensional. Opt Lasers Eng 2013;51:128–33.
8. Chen W, Chen XD, Sheppard Colin JR. Optical image encryption based on coherent diffractive imaging using multiple wavelengths. Opt Commun 2012;285:225–8.
9. He WQ, Peng X, Meng XF. Collision in optical image encryption based on interference and a method avoiding this security leak. Opt Lasers Technol 2013;47:31–6.
10. Sui LS, Xin MT, Tian AL. Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain. Opt Lett 2013;38:1996–8.
11. Lu DJ, He WQ, Peng X. Optical image encryption based on a radial shearing interferometer. J Opt 2013;15:105405.
12. Yuan S, Zhang T, Zhou X, Liu XM, Liu MT. Optical authentication technique based on interference image hiding system and phase-only correlation. Opt Commun 2013;304:129–35.