IMAGE ENCRYPTION AND STEGENOGRAPHY BASED ON COMPUTATIONAL SINGLE PIXEL IMAGING

by

Hossein Ghanbari-Ghalehjoughi

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Computer Science

at

The University of Wisconsin-Milwaukee

December 2019

ABSTRACT

IMAGE ENCRYPTION AND STEGENOGRAPHY BASED ON COMPUTATIONAL SINGLE PIXEL IMAGING

by

Hossein Ghanbari-Ghalehjoughi

The University of Wisconsin-Milwaukee, 2019
Under the Supervision of Professor Zeyun Yu

Multiple layers of information security are introduced based on computational ghost imaging (CGI). We show, in the first step, that it is possible to design a very reliable image encryption scheme using 3D computational ghost imaging with two single-pixel detectors sending data through two channels. Through the Normalized Root Mean Square scale, it is then shown that a further level of security can be achieved by merging data-carrying channels into one and using a coded order for their placement in the sequence of bucket data carried by the single channel. Yet another layer of security is introduced through hiding the actual grayscale image inside another image such that the hidden image cannot be recognized by naked eyes. We then retrieve the hidden image from a CGI reconstructed image. It is shown that the proposed scheme increases the security and robustness such that an attacker needs more than 96 percent of the coded order to recover the hidden data. Storing a grayscale image in a ghost image and retrieving different intensities for the hidden image is unprecedented and could be of interest to the information security community.

To my lovely mother and father who supported me throughout this journey.

To my brother Mohsen

and my sisters Leila and Nasrin

TABLE OF CONTENTS

LIST OF FIGURES vi
Chapter 1 1
1.1 Background and problem statement 1
1.2 – Optical encryption 1
1.3 – Single Pixel Imaging (Ghost Imaging) 3
1.4 – 3D Single Pixel Imaging 5
1.5 – Encryption based on Single Pixel Imaging 7
Chapter 2 9
2 - Encryption using 3D Single Pixel Imaging 9
Chapter 3 16
3 – Encryption based on permutation of bucket data sequence 16
Chapter 4 28
4.1. Steganography and Watermarking based on Single Pixel Imaging 28
4.2. Steganography and Watermarking based on Multi-channel to Single-channel Single Pixel Imaging 28
CHAPTER 5 36
5. Conclusions and future works 36
References 38

LIST OF FIGURES

Figure 1 - Figure 1 – Schematics of conventional single pixel imaging using two single pixel detectors 3
Figure 2 - Schematics of conventional single pixel imaging using CCD 4
Figure 3 - Schematics of computational single pixel imaging 5
Figure 4 - Experimental setup for 3D single pixel imaging 6
Figure 5 - Results from 3D ghost imaging, 3D reconstruction, color coded depth and illuminated object by a random intensity pattern (left image from left to right) and 3D reconstruction for different angle of views resulted from shading analysis of ghost images (right) 6
Figure 6 - Color based image encryption using single pixel imaging 8
Figure 7 - The schematic illustration of the experimental setup for 2-bucket 3D ghost imaging scheme with a 3-sided object 10
Figure 8 - resulting ghost image for two bucket detectors from simulation (a and b) and experimental setup (c and d). 3D reconstruction based on pair of images for simulation (e) and experimental setup (f) 11
Figure 9 - NRMS versus eavesdropping percentage for secret keys for 4000 illuminations for simulation (a) and 2000 illuminations for experimental setup 13
Figure 10 - The attacker would get these images if half and all of the key becomes accessible 14
Figure 11 - Schematic illustration of the second layer security using encrypted bucket data sequence 17
Figure 12 - Robustness against eavesdropping checked via NRMS value, for channel one (a) and two (b) obtained experimentally for 4000 shots 18
Figure 13 - Robustness against eavesdropping checked via NRMS value when the two pictures have no similarity, for channel one (a) and two (b) obtained from simulations for 2000 shots 19
Figure 14 - Experimentally recovered images from the two-channel encryption setup in connection with figure 12 21
Figure 15 - Recovered images from simulation of a two-channel encryption setup when they carry independent data connected to figure 13 22
Figure 16 - Histograms showing the distribution of bucket values in the two channels (a) and when the differences are averaged out (b). The vertical axes illustrate the number of times a certain bucket value is measured. 23
Figure 17 - NRMS scale for encryption in a single channel setup, simulation with 3000 shots (a) and experiment with 5000 shots (b). 25
Figure 18 - Recovered images from a single channel encryption for different percentages of keys disclosed 26
Figure 19 - Examples of various arrangements for multi-channel CGI and encryption 27
Figure 20 - Schematic representation of the proposed steganography setup based on computational ghost imaging 31
Figure 21 - NRMS values for different eavesdropping percentages of random matrices and bucket sequence 33
Figure 22 - Recovered images from the two channels and the secret image for different percentages of data being revealed 34
Figure 23 - Recovered images from the two channels and the secret image for different percentages of data being revealed 35

ACKNOWLEDGEMENTS

I like to express my gratitude toward Professor Zeyun Yu for the opportunity he gave me to work on this thesis and learn from him. I like to thank Professor John Boyland for his support and guidance throughout my studies in Computer Science department which without them none of what I have now would be possible.

I like to show my gratitude toward all faculty members in Computer Science department, specially Professor Hossein Hosseini from whom I learnt a lot. I am also grateful to Professor Guangwu Xu and Professor Jun Zhang, who kindly agreed to be on my thesis committee.

Chapter 1

Introduction

1.1 Background and problem statement

In the information-based world of today, the importance of information delivery and its security is such an undeniable matter that scientists and engineers of different fields have been engaged for decades with designing more robust and secure schemes. These efforts have turned the field of information security to an interdisciplinary field of research which involves researchers from both science and engineering. In general, encryption techniques are classified into: i) private- and ii) public-private-key respectively corresponding to secure communication without and with sharing a public key between receiver and sender. In the solutions that offer security based on a shared public key alongside the private key, the information is encoded by the sender through the public key but needs to be decoded via the private key owned only by the receiver. The former category without shared public key necessitates establishment of a private channel for sharing the private key for both coding and decoding.

1.2 – Optical encryption

In the recent years, however, optical encryption methods have attracted considerable popularity due to their high-speed operation, possibility of data hiding in multiple dimensions (such as phase, wavelength, spatial frequency, or polarization) with the subsequent difficulty of unauthorized access to the protected information. Different variations of Fourier transform [1, 2], the Fresnel, gyrator and joint transforms [3, 4, 5], interference principle [6], digital

holography [7], diffractive imaging [8], and polarization encoding [9] constitute only a subset of all optical encryption techniques [10]. The proposed schemes in this community have also taken advantage of the fundamental law of uncertainty in nature to transmit the secret key by a single photon whose change of state as a result of intervention is identifiable through increased error rate in the system which lays the foundations of quantum cryptography [11].

Optical methods have also been successful in the realm of information hiding. Information hiding is not meant to replace or taken as equivalent to encryption since encryption masks the meaning of the message while information hiding is supposed to mask the communication of the message. Steganography, as a reliable candidate to serve this purpose, is used to embed an unremovable piece of information on the cover data. It is essential that the embedded information (or the hidden image) should be indiscernible to the naked eye. It is also important that the hidden information resists removal and recovers reliably when needed [12].

There are also plenty of image encryption algorithms introduced via chaotic systems [13, 14, 15, 16, 17], DNA computing [18, 19, 20], cellular automata (CA) [21, 22, 23], Brownian motion [24, 25], wave transmission [26, 27], Latin squares [28] and others where the transformation of the image into noisy or patterned cipher image is the common practice. However, cryptography by computational ghost imaging (CGI) as a special class of computational imaging encryption techniques, where optical coding is used followed by computational decoding, has made remarkable progress in the field [29].

1.3 – Single Pixel Imaging (Ghost Imaging)

Ghost images are obtained by correlating the output of a single-pixel (bucket) photodetector, which is a measure of the total transmitted or reflected light from an object, with the output from a high spatial-resolution scanning photodetector or photodetector array whose illumination has not interacted with the object according to $GI = \sum_{i=1}^{n} M_i . B_i / \sum_{i=1}^{n} M_i$ where B and M respectively denote bucket values and their corresponding random matrices. The interesting reason for the use of the term ghost image lies behind the point that the image is constructed by detectors which are not individually able to reproduce an image since the bucket detector has no spatial resolution and the detector of high spatial-resolution never receives any light that has interacted with the object [30].

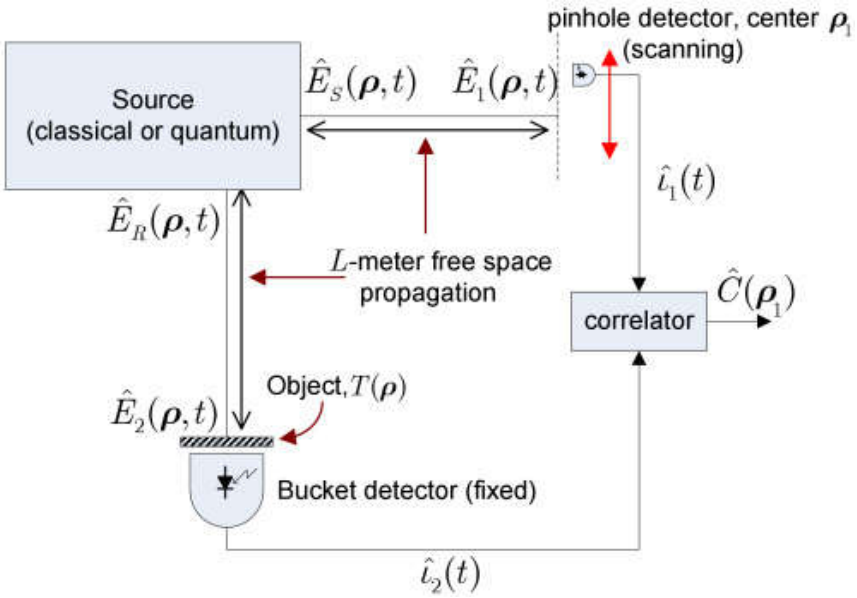

Figure 1 - Figure 1 – Schematics of conventional single pixel imaging using two single pixel detectors (one as bucket detector and stationary and other one scanning) [65]

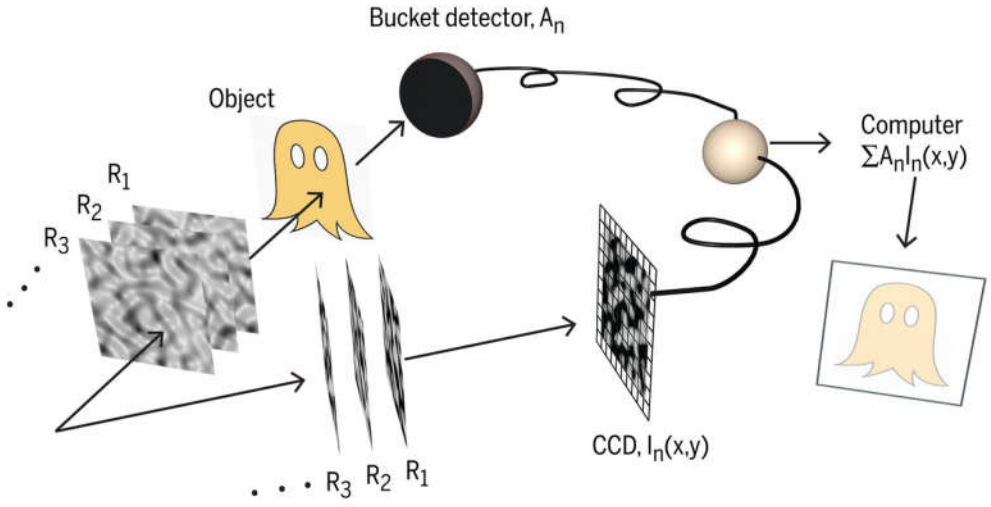

Figure 2 - Schematics of conventional single pixel imaging using CCD [66]

In classical GI a Charge Coupled Device (CCD) and a reference arm are used for reconstruction of an image whereas in computational ghost imaging, images can be obtained by a single pixel bucket detector and through controllable illumination [31, 32, 33]. In this scheme, an arrangement of lenses expands the laser beam before reaching the Spatial Light Modulator (SLM) where it takes on the intensity pattern of the SLM. Since the intensity pattern loaded on the SLM is programmed by the user, the presence of the CCD and reference arm to record the intensity pattern is unnecessary. From the time of its introduction, many attempts have been made to improve the performance of algorithms and resolve limitations alongside proposing diverse applications [34, 35, 36, 37, 38].

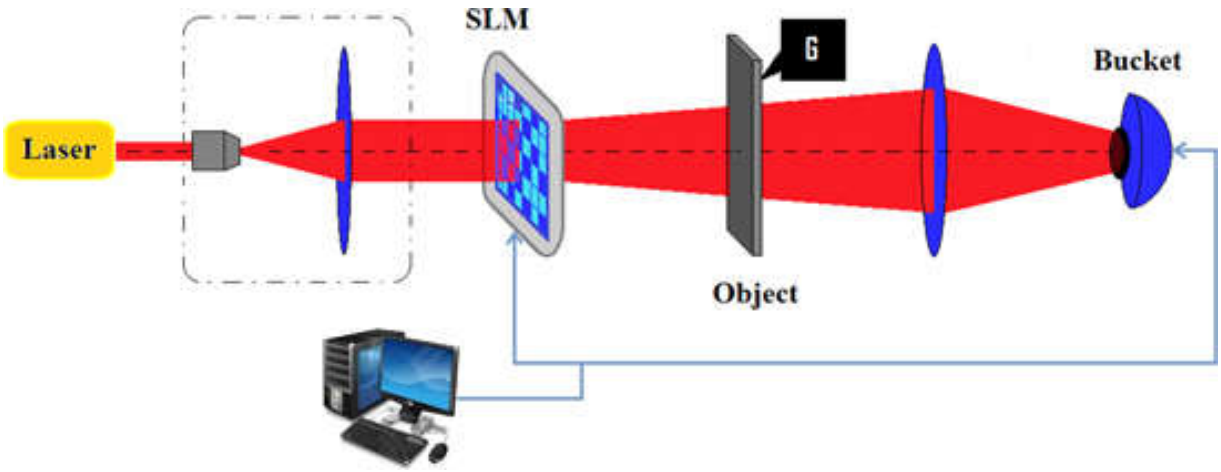

Figure 3 - Schematics of computational single pixel imaging [44]

1.4 – 3D Single Pixel Imaging

Further advancement of CGI has been achieved by computational reconstruction of 3D image of an object where several single-pixel detectors in different locations are used instead of several illuminating sources. By illuminating the object with a series of known random patterns and then measuring the backscattered light in different directions, Sun et. al. reported the possibility of capturing the 3D form of the object using four single-pixel detectors [39]. It works based on the idea that when the single-pixel detectors placed in different locations receive the reflected light and reconstruct 2D images, it resembles the case where the object is illuminated from different directions. The shading of the 2D images is then used to extract surface gradients enough for reconstruction of the 3D object.

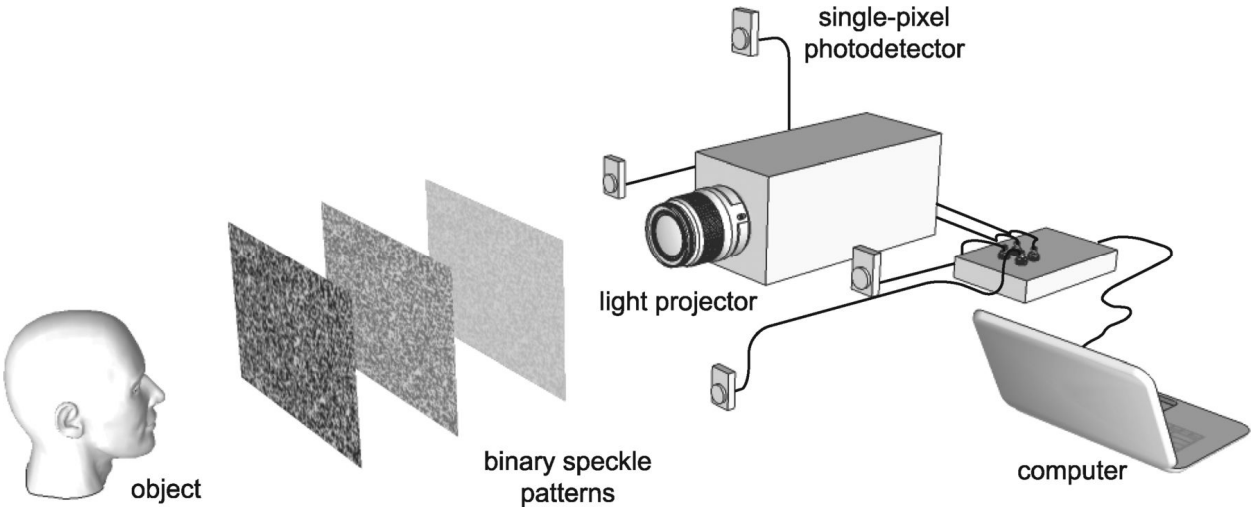

Figure 4 - Experimental setup for 3D single pixel imaging [39]

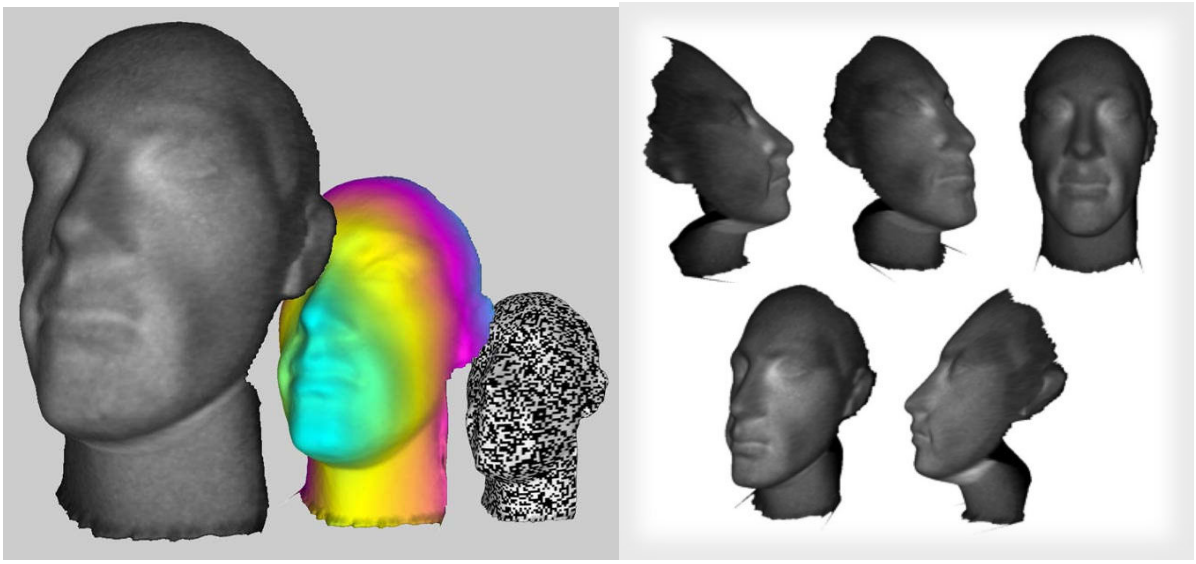

Figure 5 - Results from 3D ghost imaging, 3D reconstruction, color coded depth and illuminated object by a random intensity pattern (left image from left to right) and 3D reconstruction for different angle of views resulted from shading analysis of ghost images (right) [39]

1.5 – Encryption based on Single Pixel Imaging

CGI has also been shown to be very effective in designing optical encryption systems, for instance, in [40] Clemente et. al. has discussed the possibility of encrypting and transmitting object information to a remote party and founded the basics of CGI based encryption. In their scheme, the sender encrypts the image with the aid of an optical system similar to that used in CGI. A spatially coherent monochromatic laser beam passes through a SLM, which imposes a random intensity distribution on the beam. The modified beam illuminates the object, and the transmitted light is collected by a single-pixel detector. This operation is repeated N times for N different intensity profiles, $I = I_i(x, y)$, each of them corresponding to one secret key component, S_i. Thus, the object information is encoded in a vector of N components containing the corresponding intensity values detected by the single-pixel detector.

Next, these values are shared with the receiver using a public channel (i.e., not necessarily secure), who shall decrypt the image using a proper combination of the intensity profiles, $I = I_i(x, y)$, obtained from the privately shared secret key with the measured values by the single-pixel detector. Since then, several CGI based optical coding techniques have been reported which more or less use the same basic idea [42, 43, 44]. For example, in a paper by one of the authors [42] an improvement was realized in the security of the encrypted ghost images by using three channels of bucket data associated with the colors engaged [45, 46].

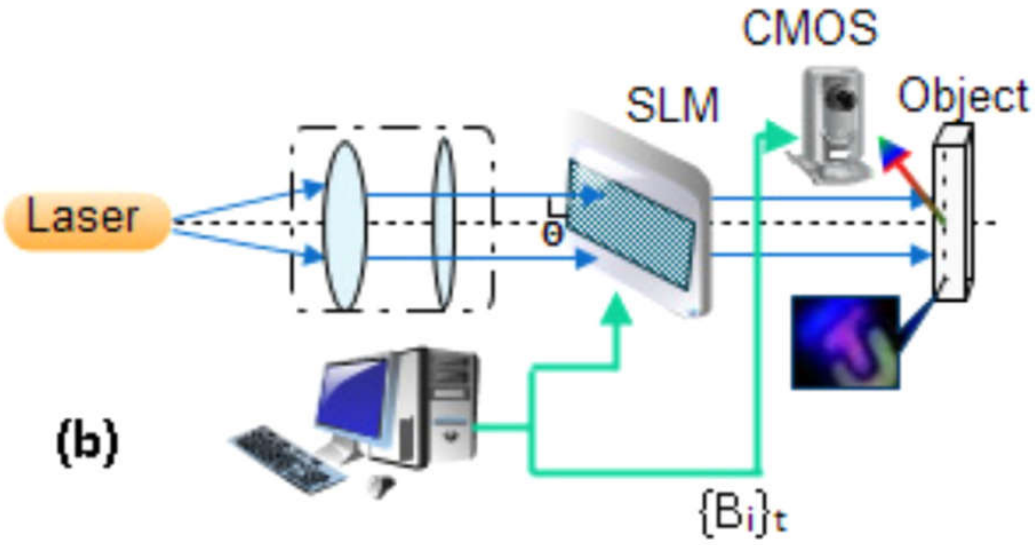

Figure 6 - Color based image encryption using single pixel imaging [42]

Other methods of optical security have also been reported based on ghost imaging where one can hide certain forms of information [47, 48, 49, 50]. In this respect, CGI compares to compressive sensing (CS) where both sampling and compression can be performed simultaneously to reduce the sampling rate at the cost of a high computation complexity at the reconstruction stage. CS can sample, compress and encrypt the image simultaneously and the measurement matrix can be taken as an encryption key. Some image compression and encryption algorithms using CS have been proposed in [51, 52, 53, 54, 55, 56, 57, 58, 59, 60].

For the aim of quantitative comparisons, a metric known as Normalized Root Mean Square (NRMS) is normally employed in these schemes to check the robustness of the encrypted ghost image under eavesdropping which, in fact, measures the amount of the error that an attacker would be faced with if part of the secret key is revealed.

Chapter 2

Encryption in 3D: 1st layer of security

2 - Encryption using 3D Single Pixel Imaging

To be proposed here is a scheme offering the possibility of image encryption based on 3D ghost imaging which uses two bucket detectors placed in two different sides of a 3D object, each providing information from one angle of view to a 3D object. The computational process on the data provided by the bucket detectors and the random matrices sent to the SLM gives the information required for the retrieval of the 3D object's image. The fact that all the information taken from the 3D object is distributed among two channels builds the foundation of a novel encryption technique: to reconstruct the final image, one needs the values from both public channels (the two bucket detectors) to correlate with the corresponding random matrices transported through a private channel.

The same idea of distributing object information among channels can also be done by different colors (as mentioned in introduction); however, the robustness of the scheme with a 3D object is much superior since it is possible to design independent channels, unlike the scheme with colors, if the angles of view of bucket detectors do not overlap. Figure 7 shows the employment of two single-pixel detectors in two different sides of a 3D object at x3 and x4. The bucket detector at x3 receives much less light from side C than from B while it receives the most of the light from side A. This is vice versa for the bucket detector placed at x4 and details of the object can be finally retrieved by combining the information from both detectors representing two channels of data.

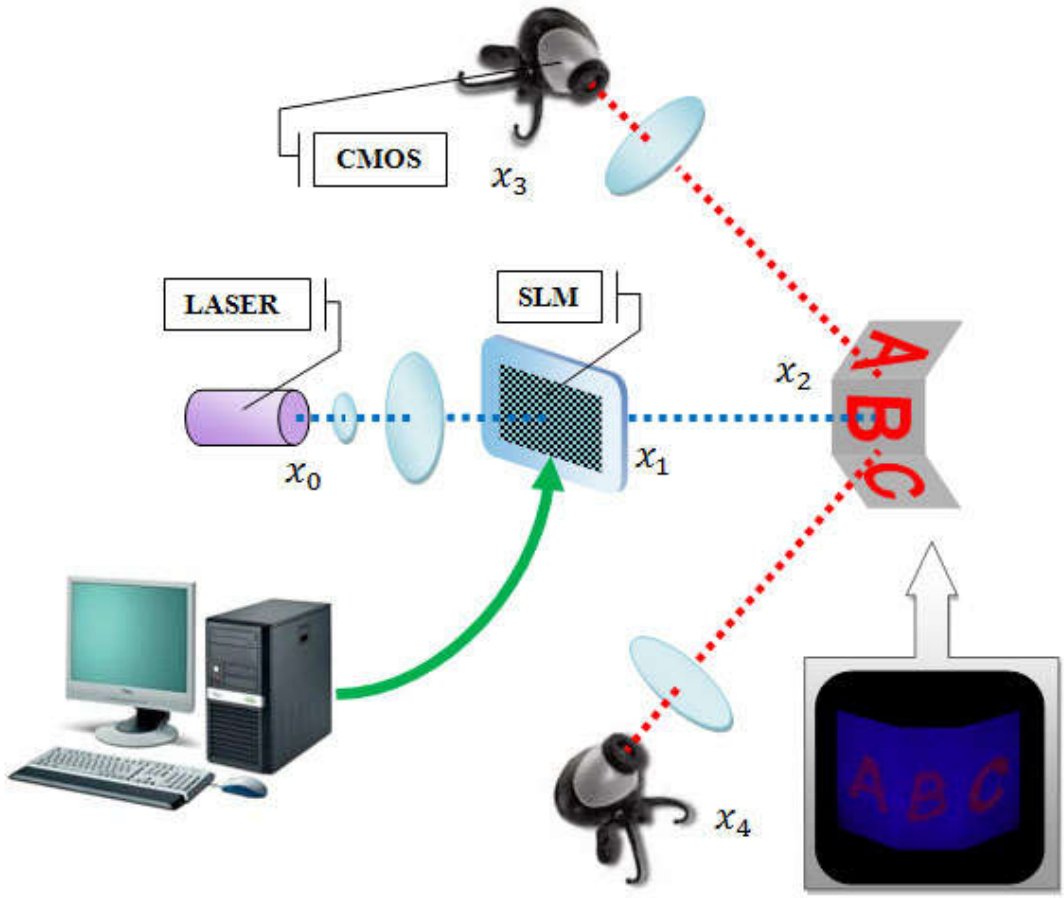

Figure 7 - The schematic illustration of the experimental setup for 2-bucket 3D ghost imaging scheme with a 3-sided object. We note that the object is fluorescent, uniformly illuminated by blue light which is depicted inside the square in the bottom right corner of the figure

The reconstructed images and 3D object extracted from them by the normalized CGI according to [41]:

$$NGI = \frac{\sum_{i=1}^{n} M_i \times \frac{B_i}{\sum_{j=1}^{n}\sum_{k=1}^{n} M_i(j,k)}}{\sum_{i=1}^{n} M_i}$$

from both simulations and experiments, are depicted in figure 8 for the two bucket detectors separately.

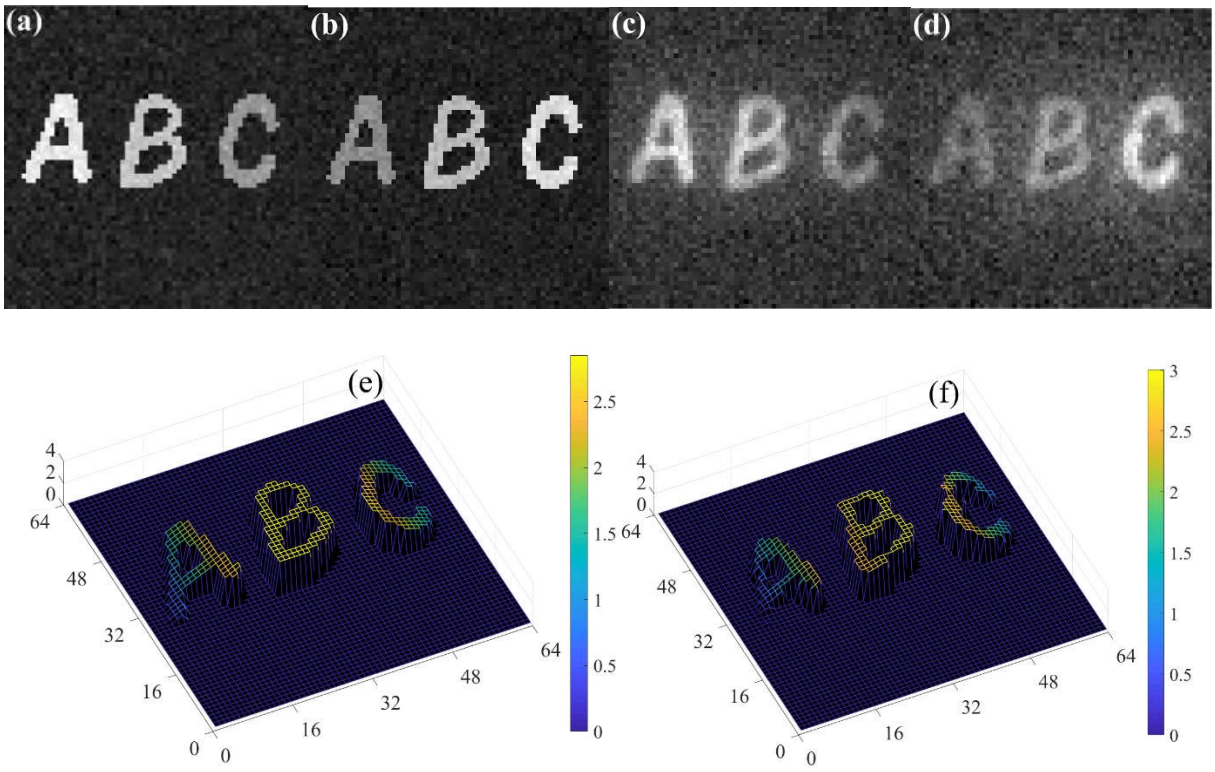

Figure 8 - resulting ghost image for two bucket detectors from simulation (a and b) and experimental setup (c and d). 3D reconstruction based on pair of images for simulation (e) and experimental setup (f)

In our proposed encryption scheme here, the light beam, after passing through the SLM and taking the random patterns loaded on the SLM, illuminates the object and the reflection is gathered by the two bucket detectors located at the two sides of the object. Each of the bucket detectors acquires information of only a portion of the object that it sees. The secret key, which is actually made up of intensity patterns $I_i(i,j)$ loaded on the SLM, is sent to the user in the form of matrices through a private channel and the two public channels carrying the information to the user contain the values detected by the single-pixel detectors.

Measuring the intensities gathered from each detector of specific range of viewing angle separately, the bucket intensities B_i comprises two channels $B_{tot} = \sum_{i=1}^{2} B_i$, where each channel is distinguished for each measurement $B_i = \{B_{i,1}, B_{i,2}, B_{i,3}, \dots, B_{i,n}\}$ and $B_{i,j}$ is the

measured bucket value for channel i and jth matrix. The final image is reconstructed by the user through correlating the B_i from two channels and the random matrices. In our experimental setup, we used Liquid Crystal (LC) based color display with 130×130 pixels as SLM. Its controller was of pcf-8833 type chip made by Phillips and its backlight system including diffractive materials and backlight LED were removed from the display. This leaves the display with two polarizers at both sides of the LC cell arrays which could be used as the transmitting SLM. We used 8-bit microcontroller ATmega32a to communicate with the pcf-8833 chip to send data to every pixel. We also made use of MATLAB to generate data for pixels as speckle pattern matrices. Then they were sent to the microcontroller through the RS-232 port of the computer. We summed up all pixels' data to have a single value for total light measured by CMOS as bucket detector's value.

The reliability of the proposed scheme for encryption of the 'ABC' 3D object is checked for each of the buckets independently and also when combined. For this purpose, we used equation 2 as the explicit form for NRMS, where I_d and I_o represent, respectively, the intensities of the decrypted and original images and n the number of shots:

$$NRMS = \frac{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{m}|I_d(i,j) - I_o(i,j)|^2}}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{m}|I_o(i,j)|^2}}$$

Figures 9 (a) and (b) show the results from simulations and experiments for the NRMS calculated when eavesdropping is done on channel one (provided only by bucket detector at x_3) and channel two (provided only by bucket detector at x_4). We should note that bucket detectors at x_3 and x_4 partially receive light from the neighboring sides too (other than the one that they have been located in front of); therefore, the contribution of those sides are naturally

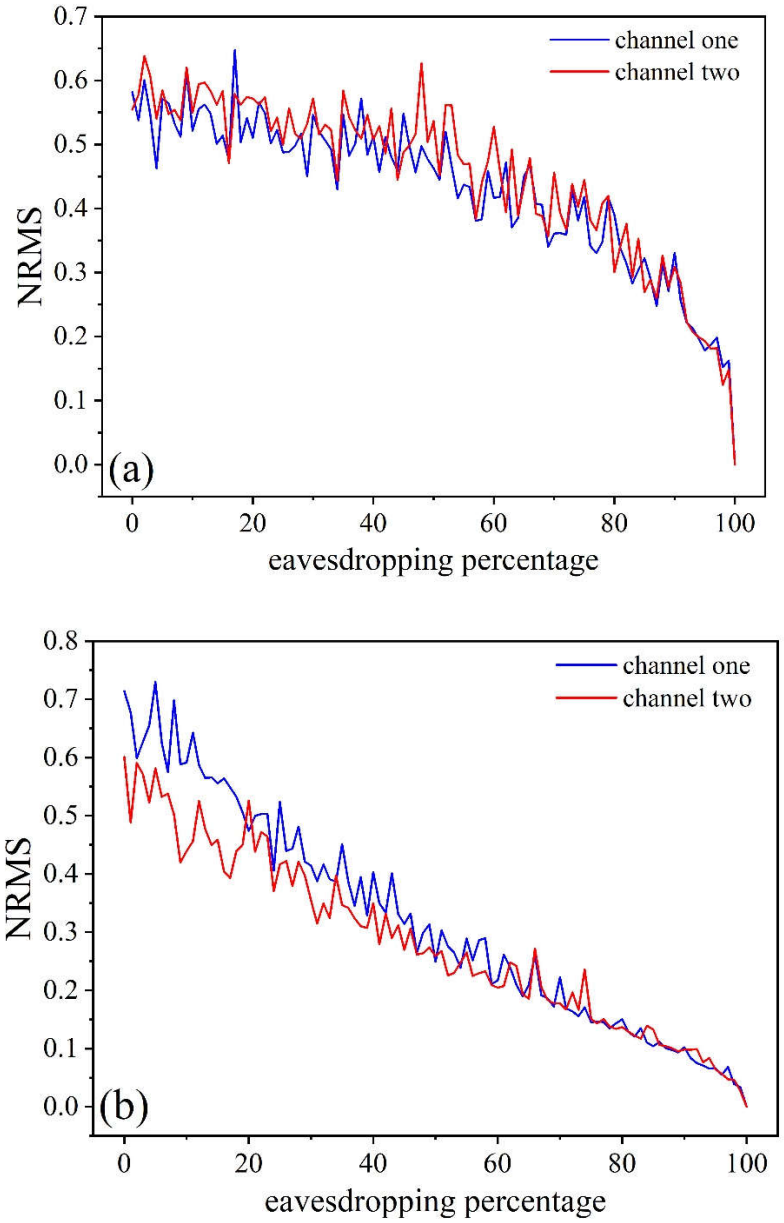

Figure 9 - NRMS versus eavesdropping percentage for secret keys for 4000 illuminations for simulation (a) and 2000 illuminations for experimental setup

included in the reported NRMS values in figure 9. As it is seen, the actual image is barley revealed even when 50 percent of the information is known to attackers. The images disclosed to the eavesdropper if 50 percent of information is revealed are shown in figure 10 which have

been obtained by simulations and checked experimentally. Also shown are the images that can be retrieved by having access to all the keys.

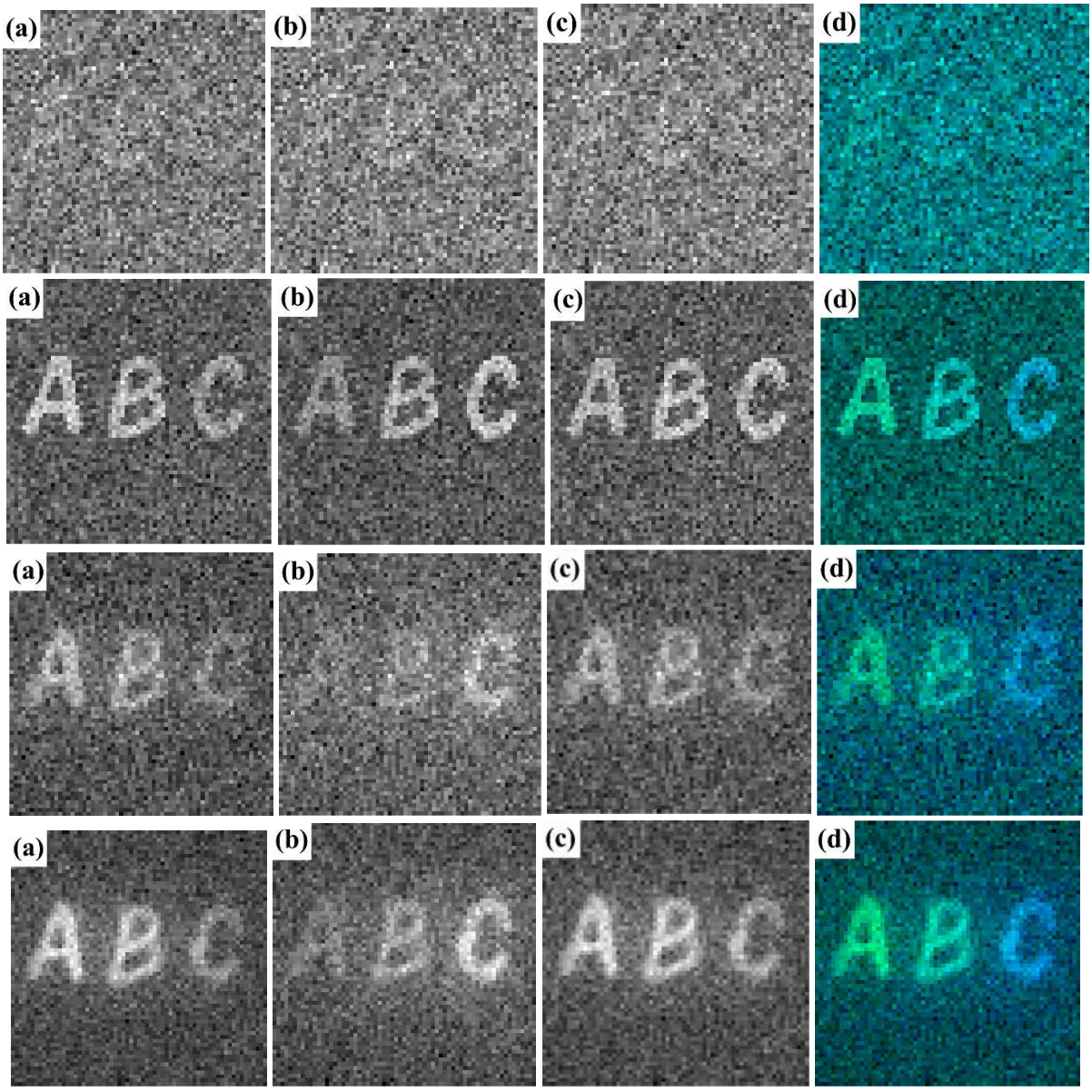

Figure 10 - The attacker would get these images if half and all of the key becomes accessible; channel x (information from detector placed at x3) (a), channel y (information from detector placed at x4) (b), channel xy (the combined information from both channels) (c) and the RG version (d). Simulation results are shown in the first and second rows respectively for 50 and 100 percent disclosure, those from experiments in the third and forth rows respectively for 50 and 100 percent disclosure. RGB images are obtained by having channel x picture as green and that of y as blue. Number of shots is the same as in figure 9. Images from simulations are obtained by 4000 shots and those of experiments by 20000 shots.

It is evident that the robustness of the scheme can be enhanced if the two detectors and hence the two channels are arranged independently of each other in the sense that there is no overlap among the information provided by each of these detectors. In such a case, the detector placed at x_3 would view half of the object and that at x_4 would view the other half with no overlap of what they see.

Chapter 3

Encryption on public data: 2nd layer of security

3 – Encryption based on permutation of bucket data sequence

The idea that gives the information another layer of security is based on the fact that sending the bucket data through multiple public channels can be made secure by combining them into one single channel of data. Depending on the number of shots and thus the number of bucket values in each of the channels, many different permutations can be used to put these bucket data in a single vector corresponding to the final single channel. The coding then can happen via ordering the sequence of the data from multiple channels and sharing privately the key for the correct sequence, see figure 11 for a schematic representation of the idea.

This layer of security is added to the one coming from randomly generated matrices since, as it will be shown here, without a prior knowledge of the right sequence of the bucket data it would be almost impossible to correlate the right bucket values with the corresponding random matrix. Although there can be many complicated functions generating complex permutations of bucket data sequence, here we have used a random distribution. Also, we used two channels and have assumed that the same number of correct buckets are found by attackers and correlated by their corresponding random matrices in both channels.

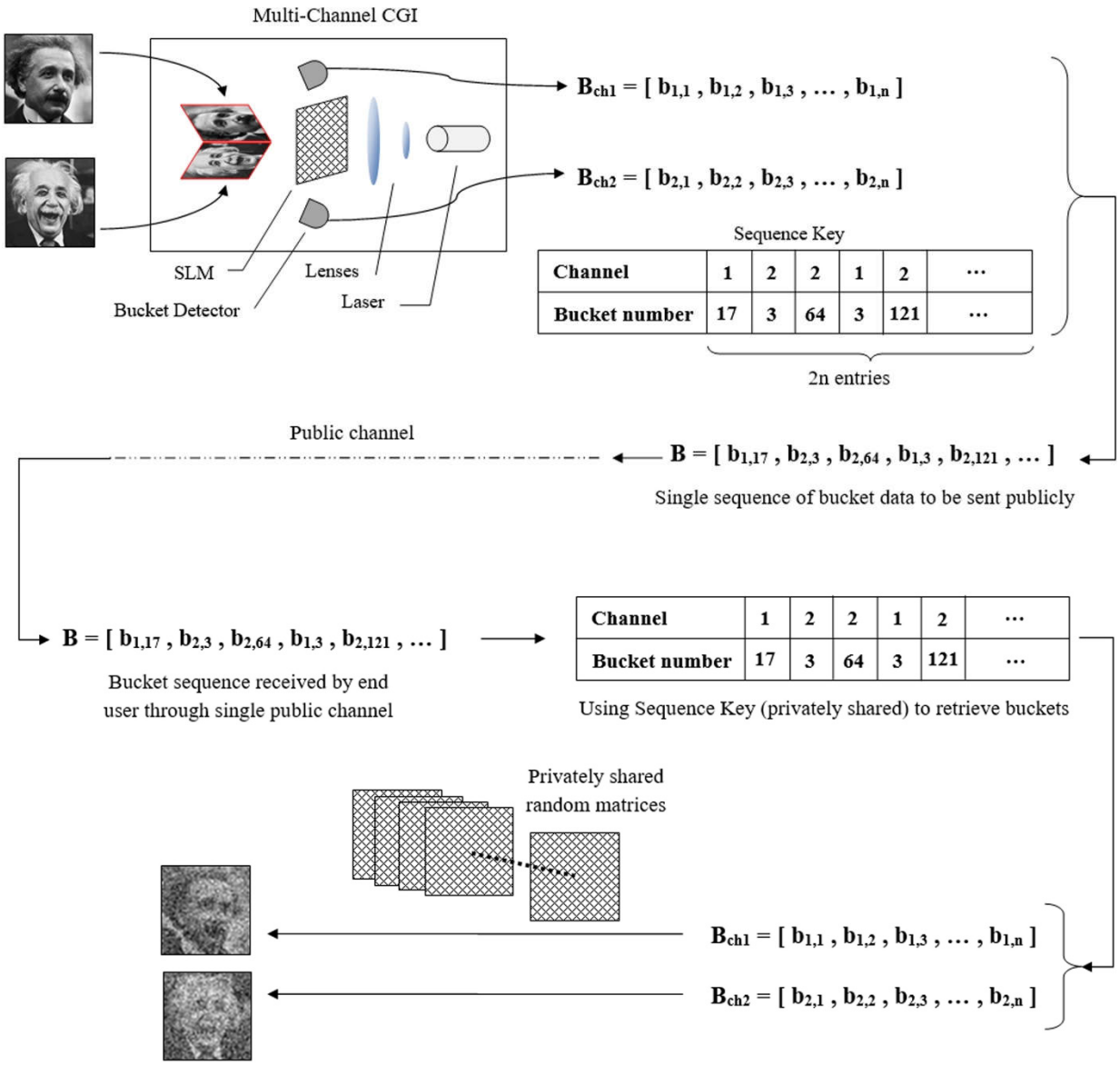

Figure 11 - Schematic illustration of the second layer security using encrypted bucket data sequence.

We introduce the second layer of security to the ABC example of section 2 where the two channels have partial overlap due to partially shared viewing angle of bucket detectors and, using the NRMS scale, compare the security degree with the case where the scheme of figure 11 is employed where two different pictures or objects are used forming independent channels of data.

Since there are two sets of encrypted data in this arrangement, one related to the random matrices (first layer of security) and the other corresponding to the buckets' data sequence, the NRMS plot gets 3 dimensions as shown in figures 12 and 13. When we compare these two figures, it is evident that when the channels carry independent data, security given by the second layer provides more resistance against attacks and NRMS value starts reduction slowly in higher eavesdropping percentages. Recovered images from the arrangements leading to figures 12 and 13 are shown in figures 14 and 15.

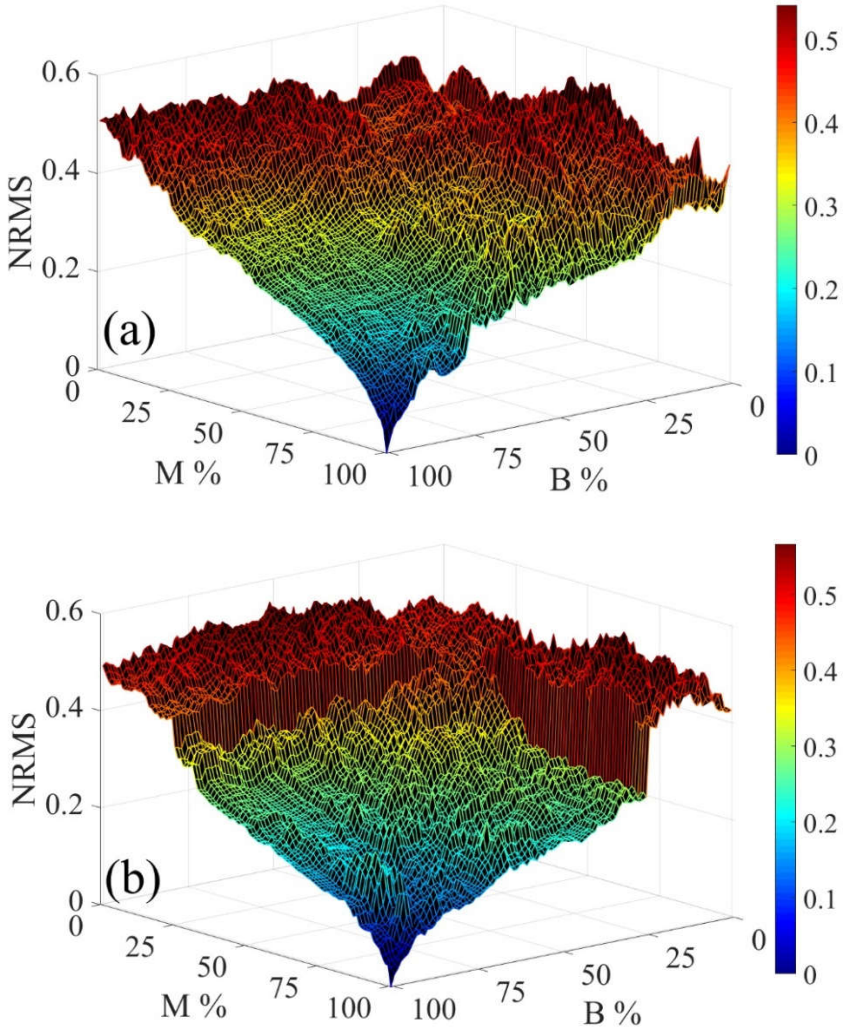

Figure 12 - Robustness against eavesdropping checked via NRMS value, for channel one (a) and two (b) obtained experimentally for 4000 shots

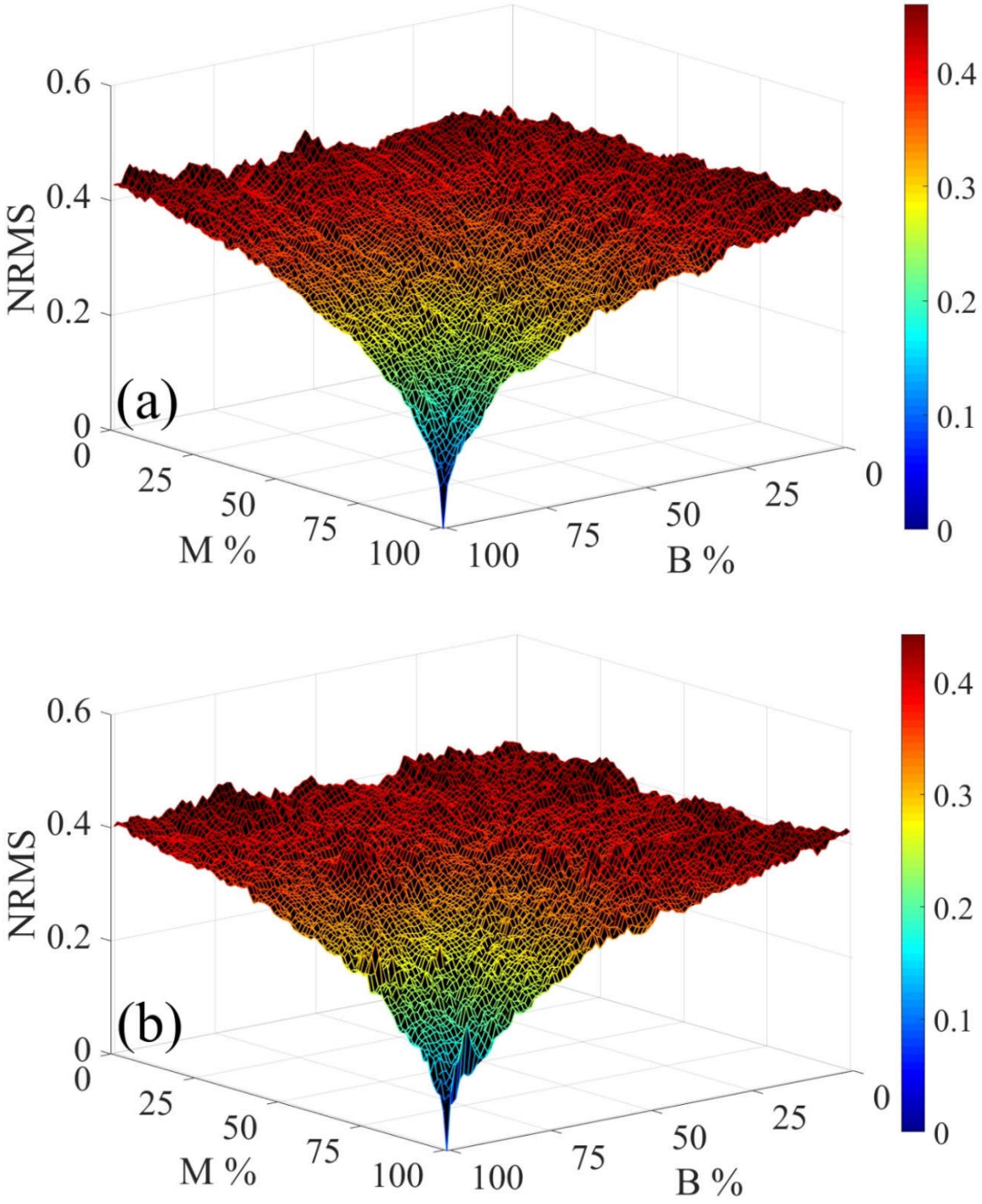

Figure 13 - Robustness against eavesdropping checked via NRMS value when the two pictures have no similarity, for channel one (a) and two (b) obtained from simulations for 2000 shots

The better security level discussed above owes itself to the differences in bucket values range for different images. Since the bucket values for different images are in different ranges, having a few wrong bucket values (i.e. the ones belonging to the other channel) ruins the image of this channel when we recover the image. However, if the attacker plots a histogram of bucket values which have been sent in a single channel, it is very easy to distinguish bucket values of a specific channel, see figure 16(a). We circumvented the problem by a simple mathematical trick: the matrices transmitted through each of the two channels are multiplied by the average of the other. Although one can use other tricks to dissipate the weight difference between the two intensity distributions, the one we employed simply puts both distributions in the same intensity value interval as shown in figure 16(b). In doing so, there is no need to change the image retrieval process since multiplying a constant to all bucket values does not change the resulting image.

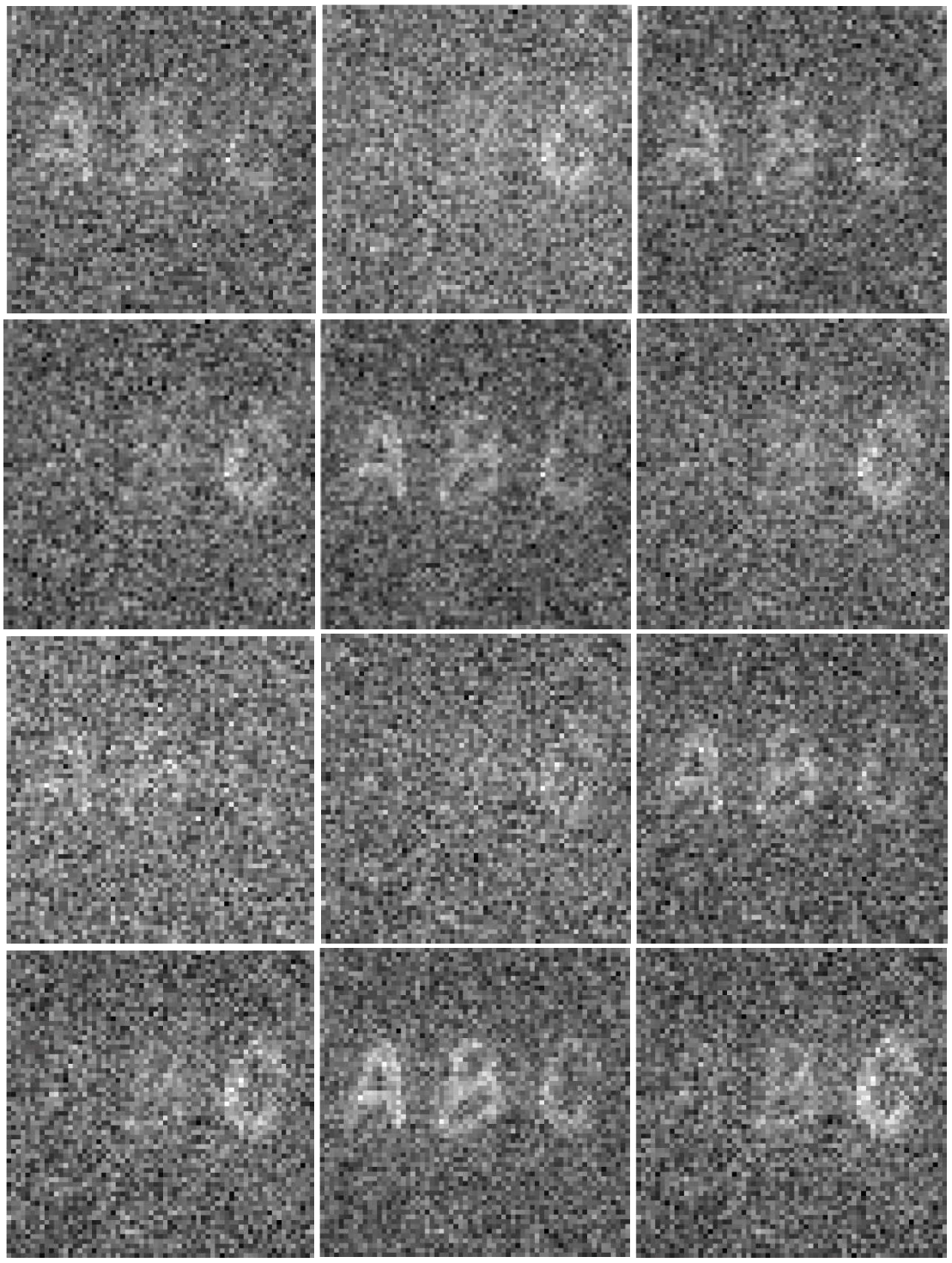

Figure 14 - Experimentally recovered images from the two-channel encryption setup in connection with figure 12. Top and second row from left to right respectively: channel one for 70, 70, 80, 100, 100, and 100 percent of random matrices revealed respectively for 70, 100, 100, 50, 80, and 100 percent of buckets disclosed. Third and last row from left to right respectively: channel two for 70, 70, 80, 100, 100, and 100 percent of random matrices revealed respectively for 70, 100, 100, 50, 80, and 100 percent of buckets disclosed

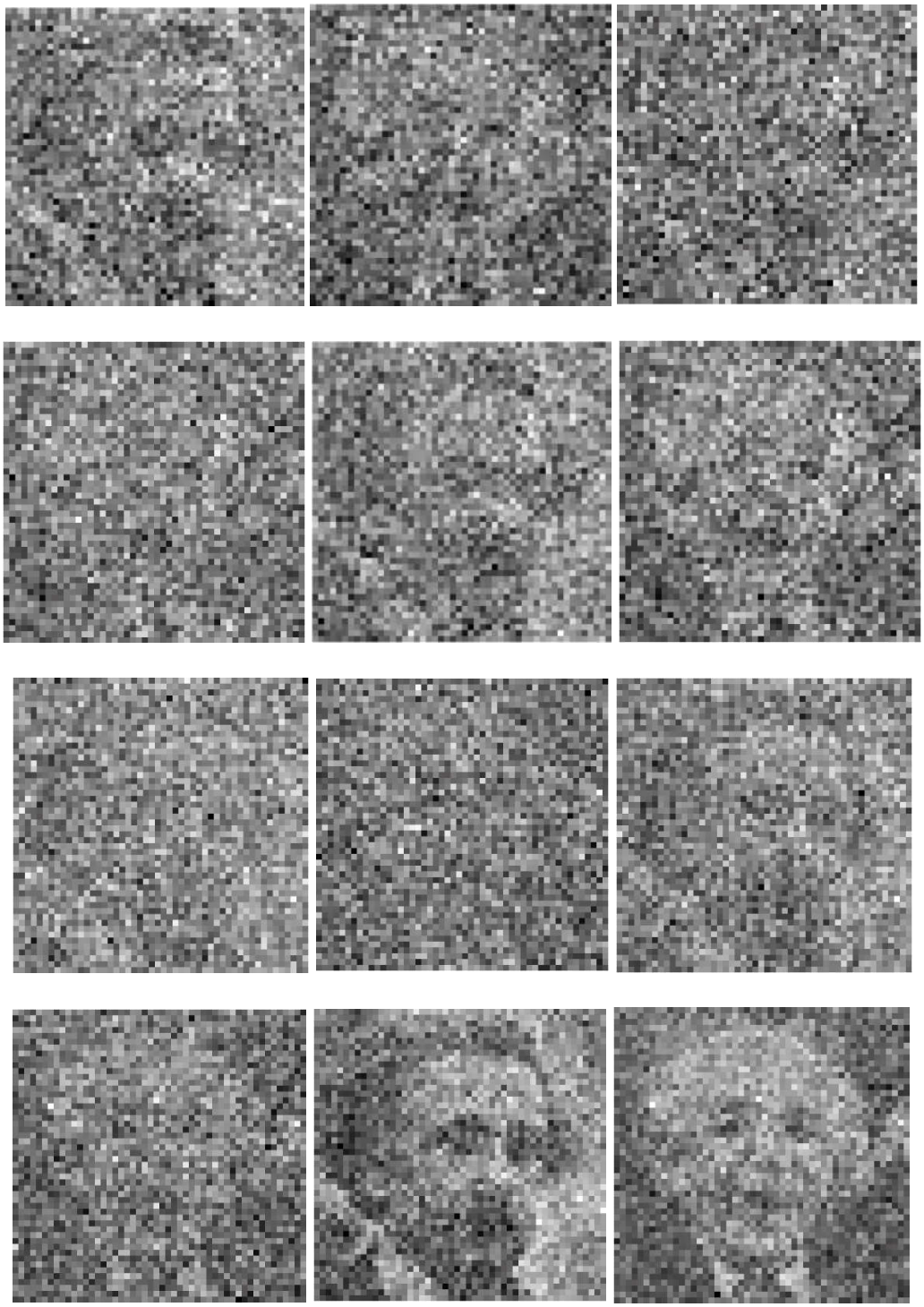

Figure 15 - Recovered images from simulation of a two-channel encryption setup when they carry independent data connected to figure 13. Top and second row respectively from left to right: channel one for 70, 50, 70, 100, 100, and 100 percent of random matrices revealed respectively for 70, 100, 100, 50, 70, and 100 percent of buckets disclosed. Third and bottom row respectively from left to right: channel two for 70, 50, 70, 100, 100, and 100 percent of random matrices revealed respectively for 70, 100, 100, 50, 70, and 100 percent of buckets disclosed

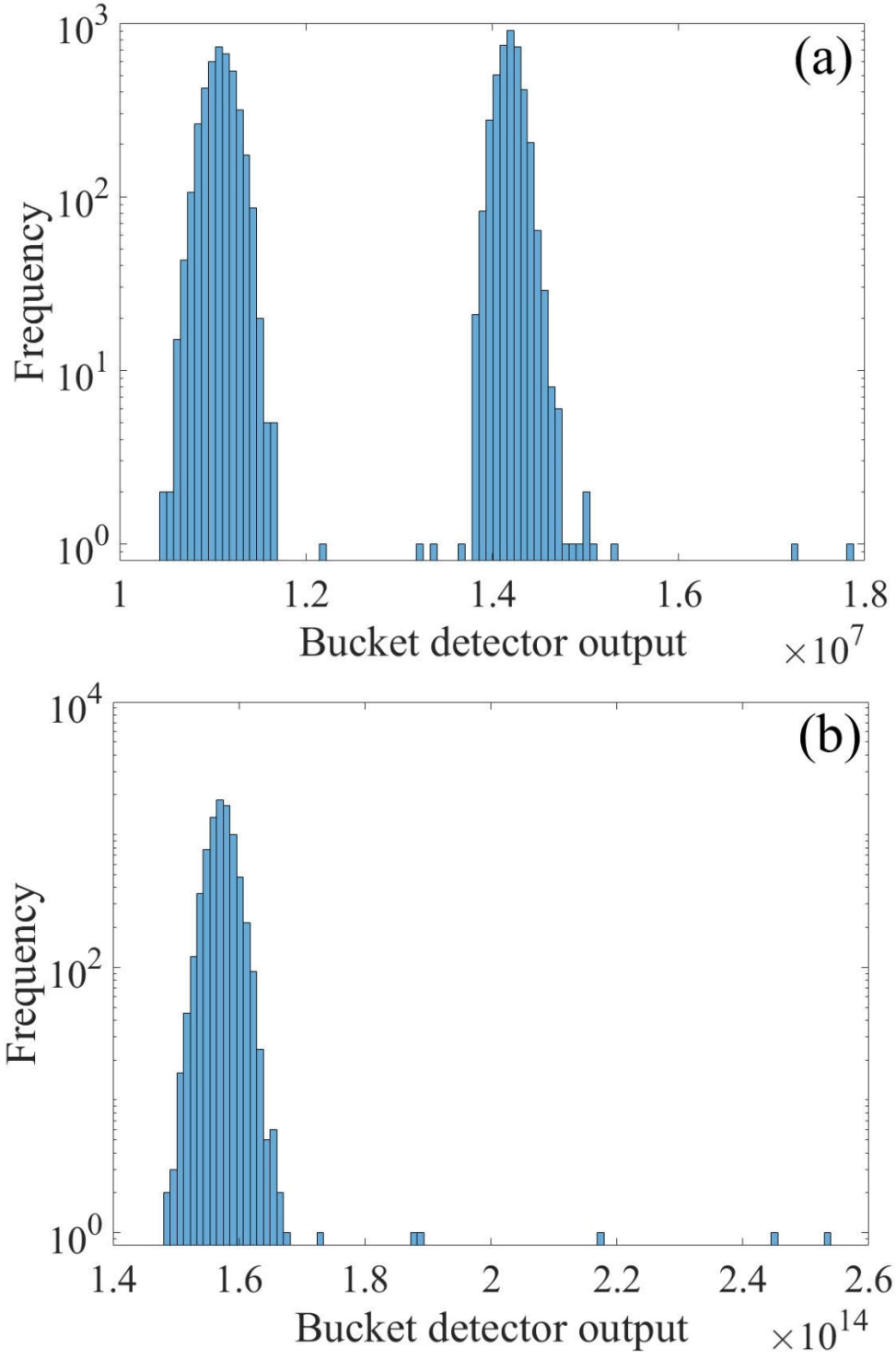

Figure 16 - Histograms showing the distribution of bucket values in the two channels (a) and when the differences are averaged out (b). The vertical axes illustrate the number of times a certain bucket value is measured.

Such an encryption on public keys can also take place in a single channel CGI setup. However, as shown in figures 17 and 18, the rate of NRMS reduction is faster as more keys are revealed. This is to say that if more channels of bucket data are involved, the security increases and it is harder to break it. As a conclusion on this chapter, we can note that the idea of multi-channel CGI used for encryption of bucket data can be done in different arrangements depending on the type of information transmitted by the channels. In figure 19, we show some examples of such multi-channel arrangements leading to the second layer security: figure 19(a) illustrates the use of multifluorescent colored object and their color-sensitive buckets in a single channel, (b) shows RGB illumination on the colored objects, (c) depicts the setup employed in the experimental part of this paper, and (d) shows how we can have multiple independent regular CGI setups or make use of a single CGI setup multiple times to generate the second layer security.

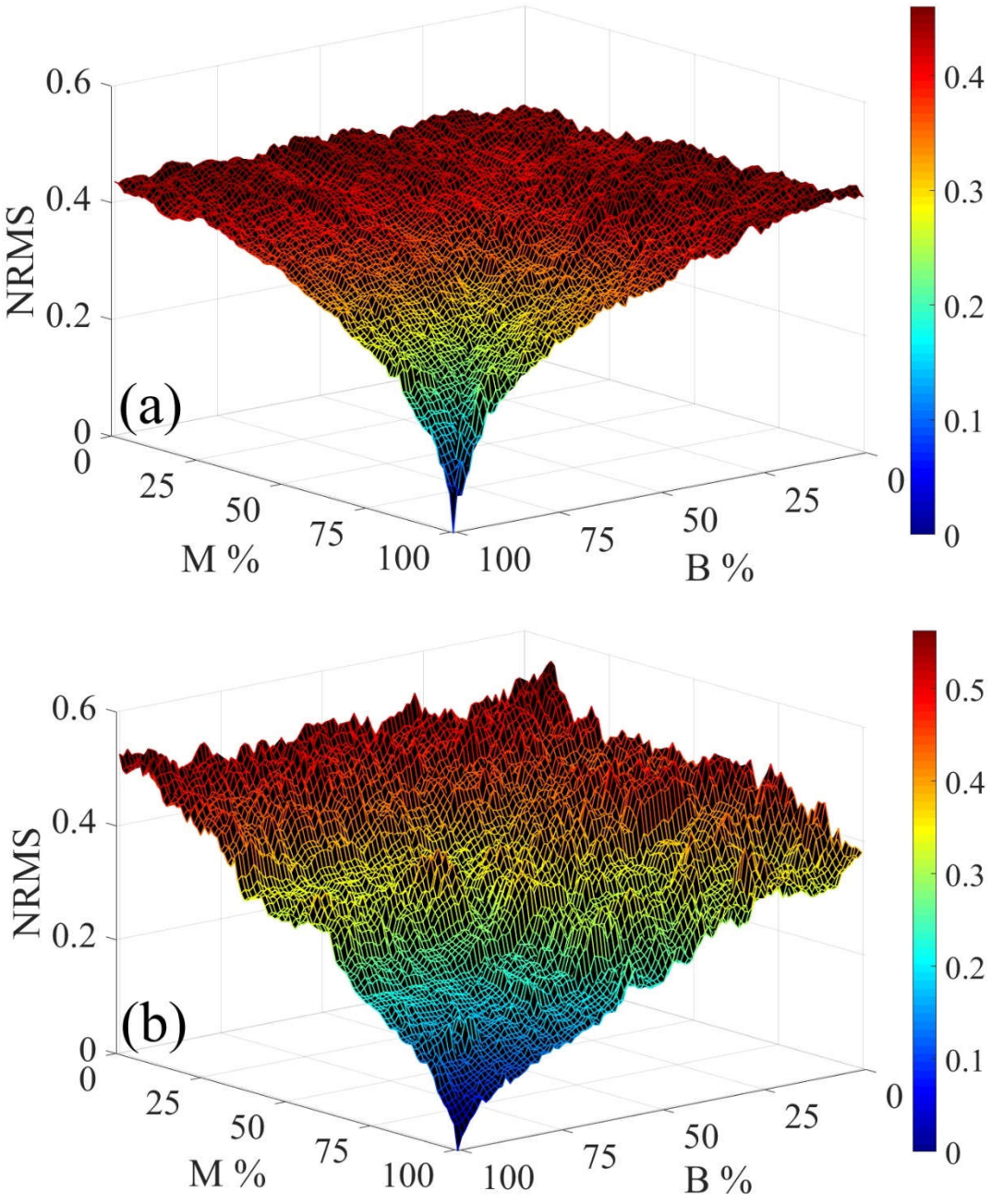

Figure 17 - NRMS scale for encryption in a single channel setup, simulation with 3000 shots (a) and experiment with 5000 shots (b).

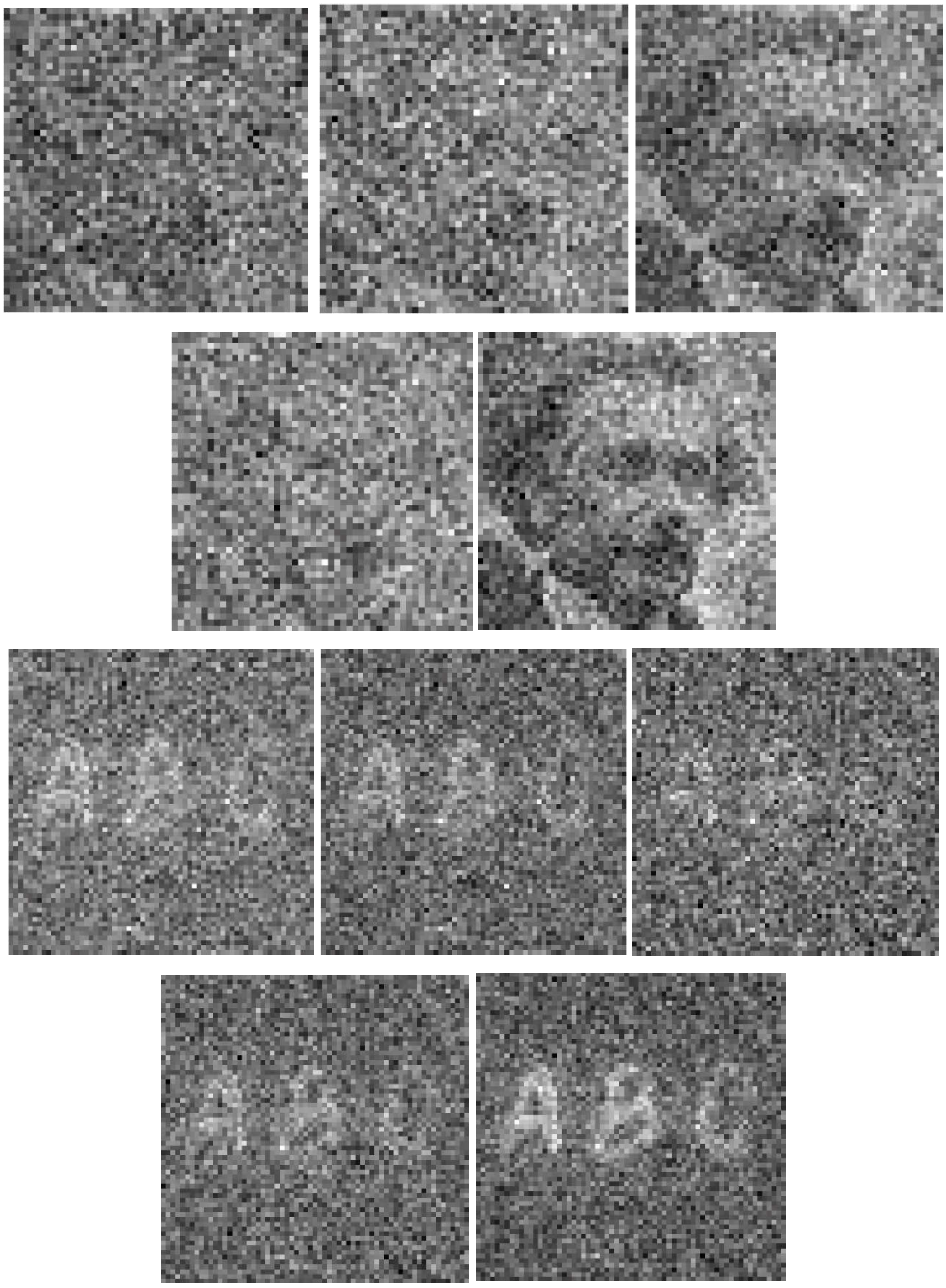

Figure 18 - Recovered images from a single channel encryption for different percentages of keys disclosed. Top and second row respectively, left to right: simulation for 55, 55, 90, 100, and 100 percent of random matrices revealed respectively for 55,100, 90, 55, 100 percent of buckets obtained. Third and bottom row respectively, left to right: experiment for 70, 70, 100, 100, and 100 percent of random matrices revealed respectively for 70,100, 50, 70, 100 percent of buckets obtained.

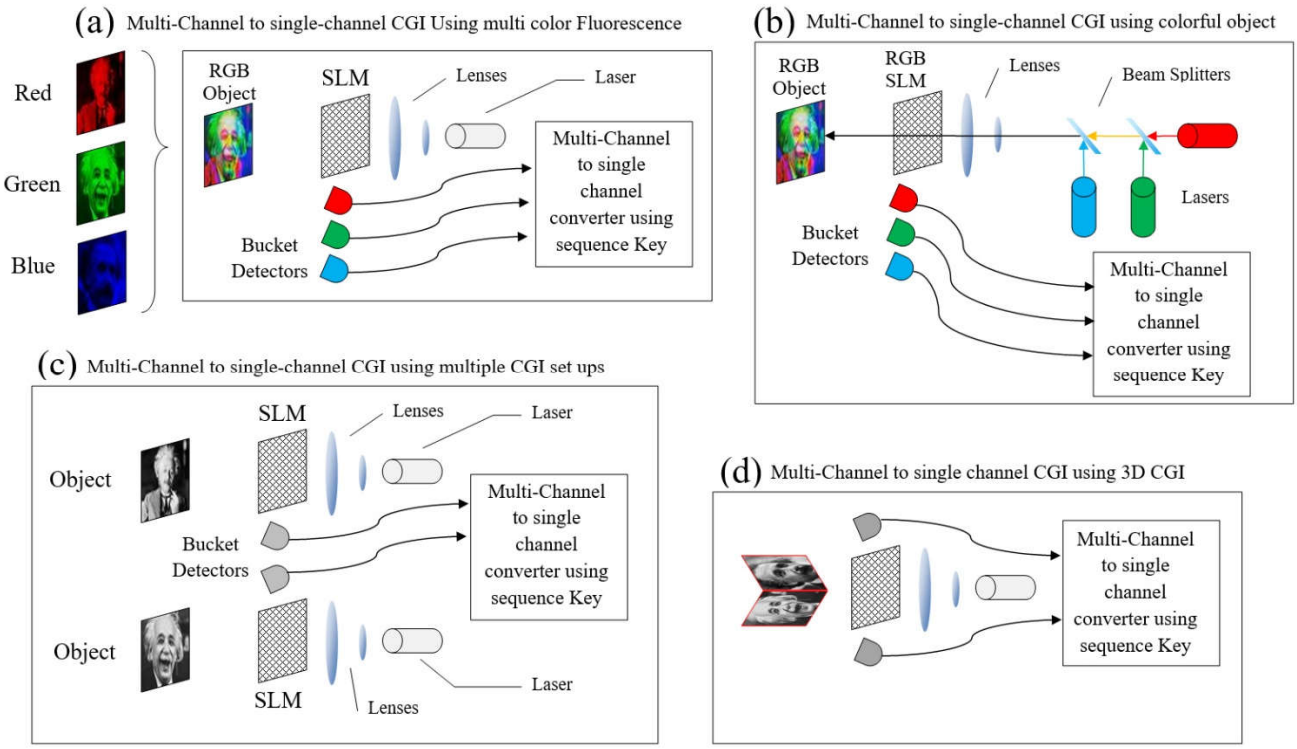

Figure 19 - Examples of various arrangements for multi-channel CGI and encryption. Top left: three different colors of RGB fluorescent object form three independent channels carrying different color-dependent intensities (the laser is single color), top right: three lasers of RGB colors are combined into one single beam illuminating an object after passing through an RGB SLM (three different colors make three channels), bottom left: two independent CGI setup for different objects but the same random matrices (bucket data of each setup constitute the channels), bottom right: a 3D object for which multiple bucket detectors are used for different sides (range of view angles that each bucket sees make the channels)

Chapter 4

Steganography: 3rd layer of security

4.1. Steganography and Watermarking based on Single Pixel Imaging

The interesting idea of watermarking corresponding to hiding an image inside another is also shown to be applicable in CGI. In [47], a high security level is achieved by demonstrating that an object and multiple hidden marks can be simultaneously recovered using only one rebuilt reference intensity sequence in ghost imaging. Watermarking encryption based on GI in later works led to the achievement that eavesdropping less than 45 percent on secret keys composed by random speckle patterns cannot retrieve the watermark image with the second-order correlation algorithm [48]. Previous attempts for optical image hiding include Double Random Phase Encoding (DRPE) [61], off-axis holography system [62], phase shifting holography system [63], cascaded phase only mask architecture [64], and Joint Transform Correlator (JTC) [65]. A comprehensive review on these techniques can be found in [50].

4.2. Steganography and Watermarking based on Multi-channel to Single-channel Single Pixel Imaging

In this chapter, we see that the idea can be realized by a two-channel CGI setup introduced in the previous chapter. We call the host image, cover image and the hidden one, secret image. In our proposed configuration, one of the two mentioned channels carry the information for cover image and the other channel carries the almost identical image to first channel. The image that Second channel carries is the weighted combination of secret image and cover image. We

multiply the secret image by small factor like 0.15 and then add it to cover image. Now we have two almost identical images for two channels. If we use the multi-channel to single-channel system introduced in previous chapter, it is very hard for attackers to distinguish if the public keys (bucket values) are related to a single-channel or multi-channel as the data in both channels are for almost identical images. In retrieval process for the image in single pixel imaging, the basic and simplest formula is:

$$Image = \frac{\sum_{i=1}^{n}(M_i \times B_i)}{\sum_{i=1}^{n} M_i}$$

Since the two images going through the CGI process are almost identical, the term inside the summation for both images will result to almost identical images in such a way that one can use $M_i \times B_i$ of one image and add it to the summation of the other image and it would increase the SNR of final image. However, if we do the same thing for two very different images, using $M_i \times B_i$ from one image in reconstruction process of the other one will reduce the SNR. This will mislead the attackers that they are recovering the real and only image. So, if they find the correct matrices and their corresponding buckets and do the summation over their $M_i \times B_i$ multiplications, only the cover image will emerge. Since we send all bucket data to the receiver through an encrypted order in the single channel provided by combining the two channels, it is almost impossible to realize that the sequence contains the information of two images. Based on our simulations, the attacker needs to correctly identify more than 96% of the buckets and matrices in order to retrieve the secret image.

The ultimate level of security is then introduced by the fact that without the private key of the correct permutation of bucket data sequence, attackers will always retrieve the same cover image (assuming that they correctly find and multiply random matrices and their corresponding bucket values) which makes it hard to guess that there can be a hidden image discoverable by subtraction of those two images from the two channels. The reason for the difficulty is twofold: on one hand, ghost images are always noisy and, on the other hand, the two images are very similar to each other thus the attacker needs to identify the exact matrices and corresponding buckets in order to be able to reconstruct the secret image. Although it is possible to find the corresponding bucket for each matrix, they will get the cover image in any summation of those bucket-matrix multiplication pairs. There is just one correct combination and we show that the attackers need to discover more than 97 percent of buckets' values' sequences in order to be able to obtain the hidden image. A schematic illustration of the proposed setup is shown in figure 20.

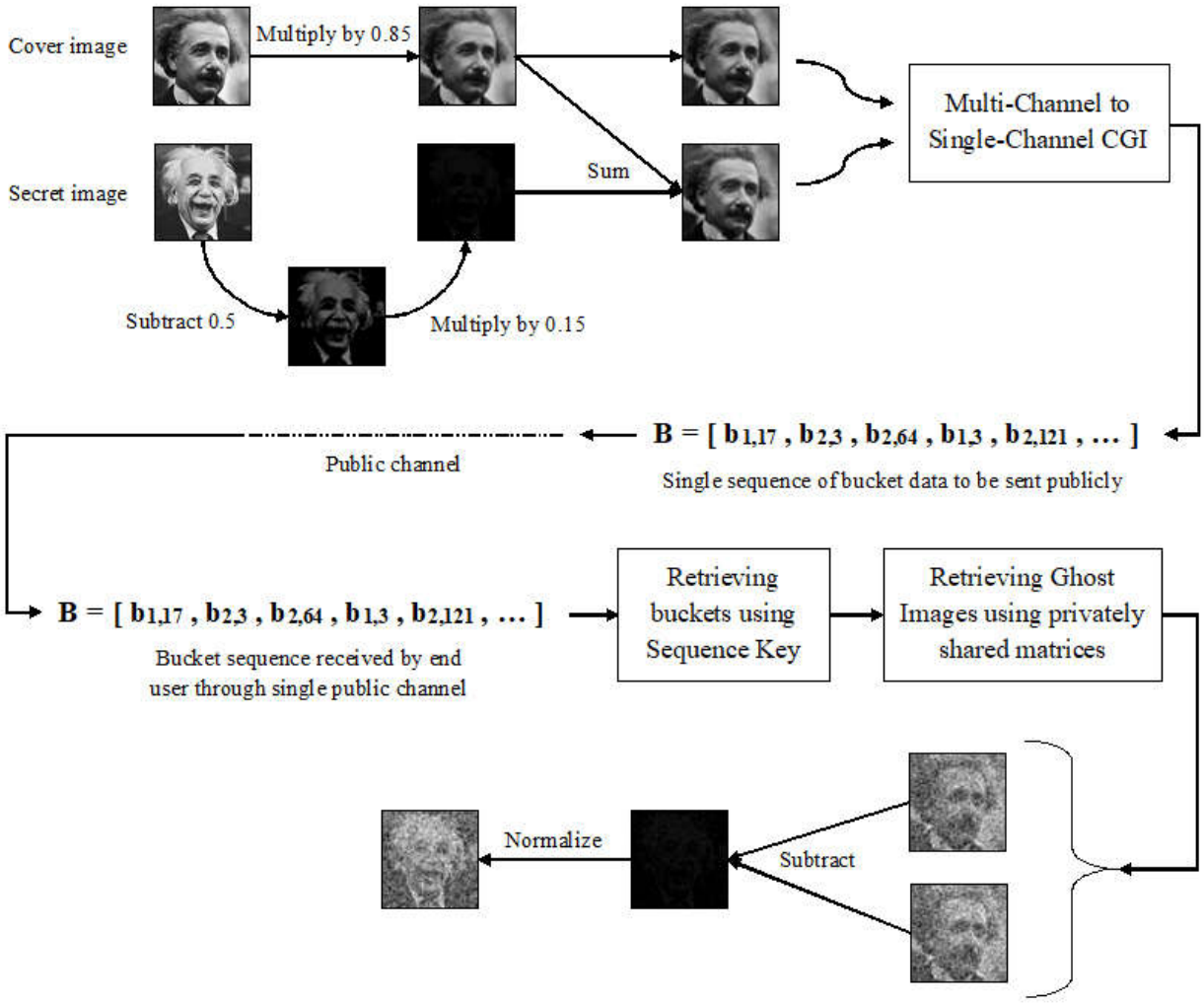

Figure 20 - Schematic representation of the proposed steganography setup based on computational ghost imaging

To show the applicability of the scheme, we used a straight-face and a laughing-face Einstein portraits respectively as the cover and secret images. Both channels transmit the cover image (straight-face Einstein) but the one carried by channel two is added by a small fraction of the secret image (laughing-face Einstein). The robustness of the technique is checked via the NRMS metric for different percentages of random matrices and bucket data disclosure. It is seen from

figure 21(a-c) that the recovery of the secret image is almost impossible unless more than 97 percent of bucket data sequence is correctly found for more or less the same number of random matrices being revealed to the attacker. It should also be noted that for 100 percent of bucket data sequence disclosed to attackers, they need to get access to almost 50-60 percent of random matrices.

The images from simulations are also depicted in figure 22 and 23 for different eavesdropping percentages. The left row shows the recovered image of channel one (cover image), the middle row belongs to the reconstructed image of channel two (secret image embedded in the cover), and the right row illustrates those of the retrieved secret image (by subtraction). It is noted that some basic conditions have been met in the proposed CGI-based steganography which guarantee the robustness and feasibility of the scheme: the cover image was not degraded after embedding the secret image, the secret image was not perceptible from the final "cover + secret" image, and the robustness of the secret image was not damaged after being embedded.

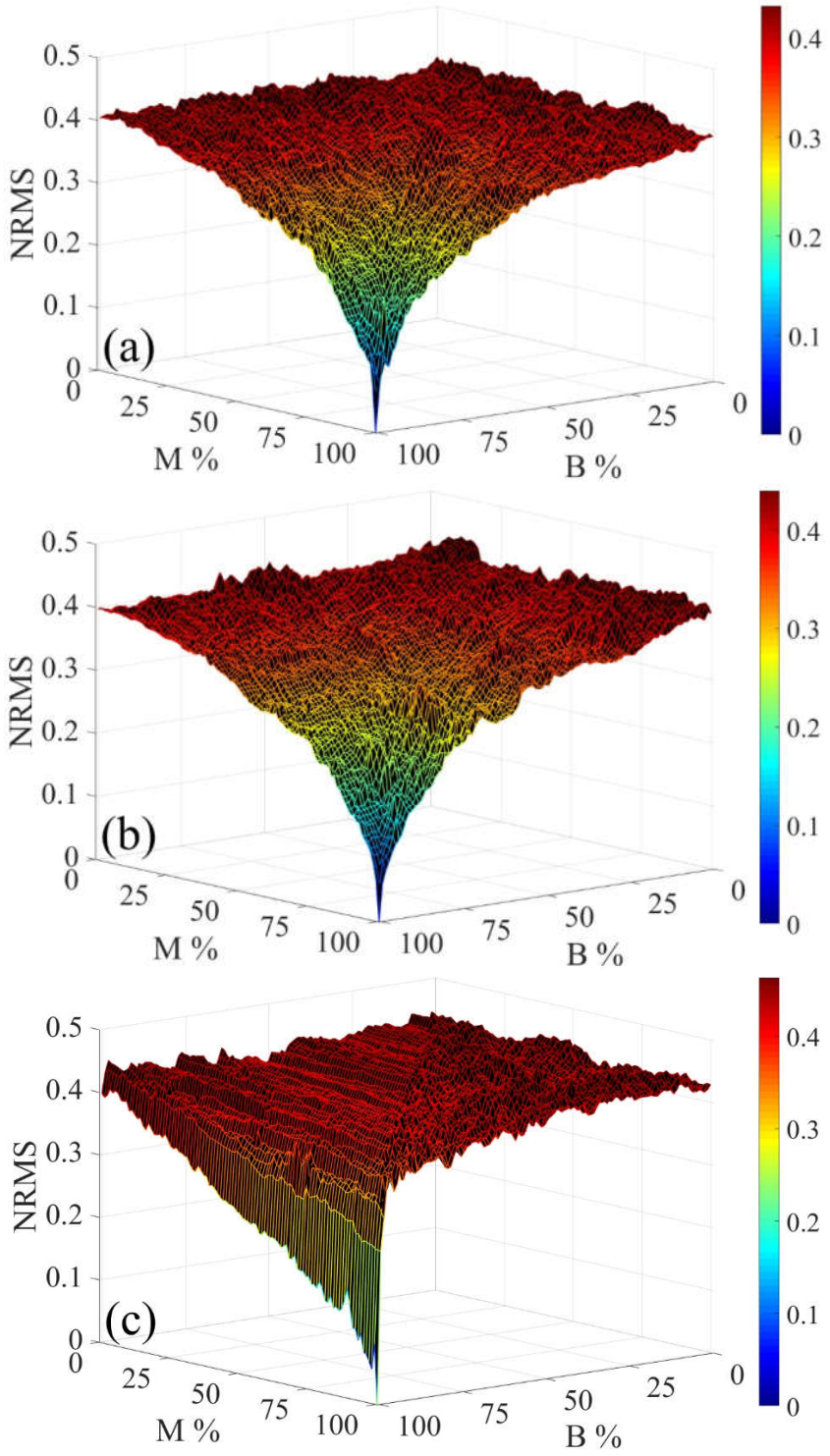

Figure 21 - NRMS values for different eavesdropping percentages of random matrices and bucket sequence; cover image of channel one (a), cover image multiplied by a fraction of secret image of channel two (b) and secret image (c). Number of shots is 3000

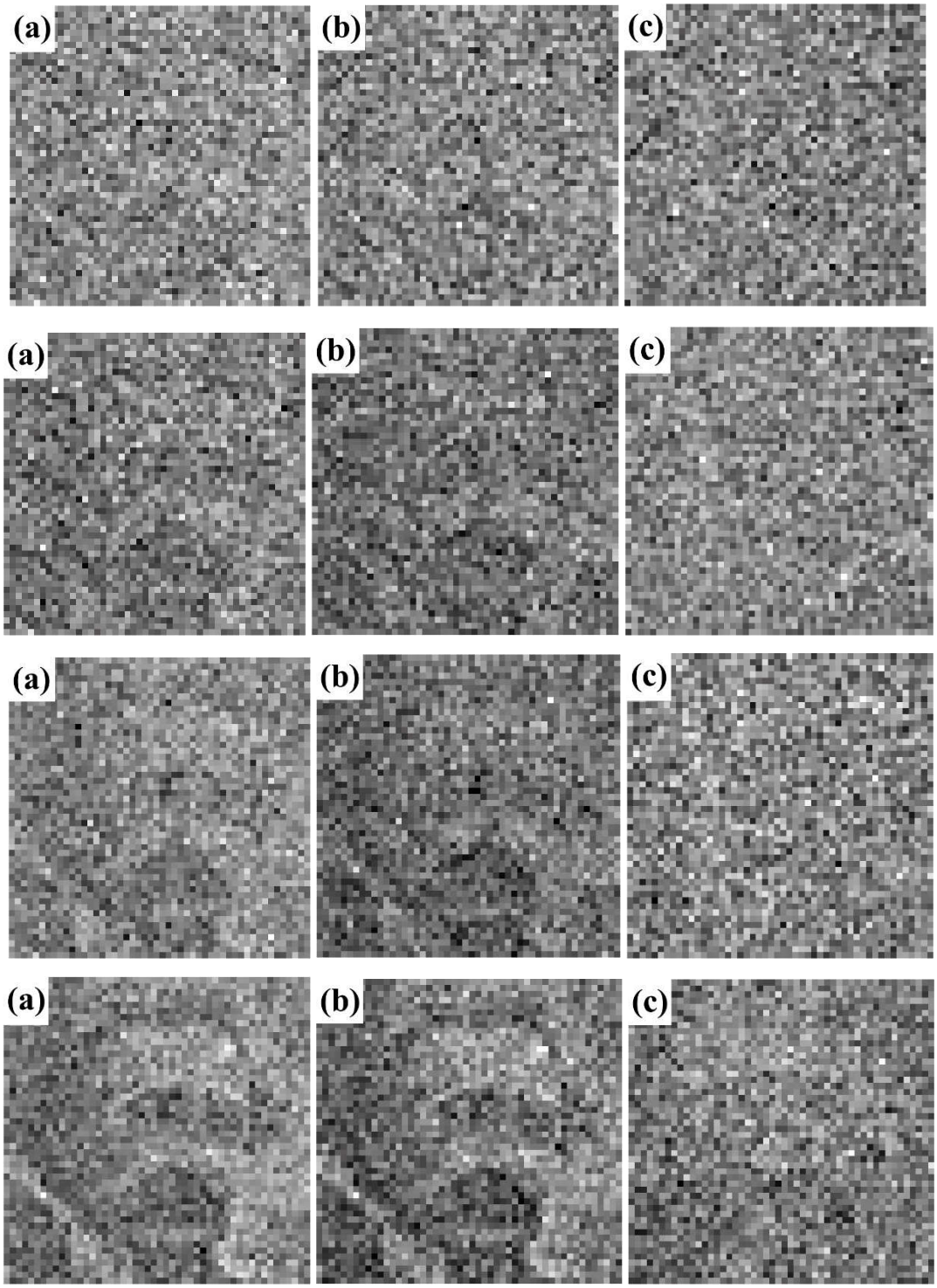

Figure 22 - Recovered images from the two channels and the secret image for different percentages of data being revealed. Cover image (channel one) (a), secret image embedded in cover image (channel two) (b), and secret image (c). Percentages of data disclosure from top to bottom for random matrices and buckets respectively are: 50-50, 65-65, 80-80, 96-96.

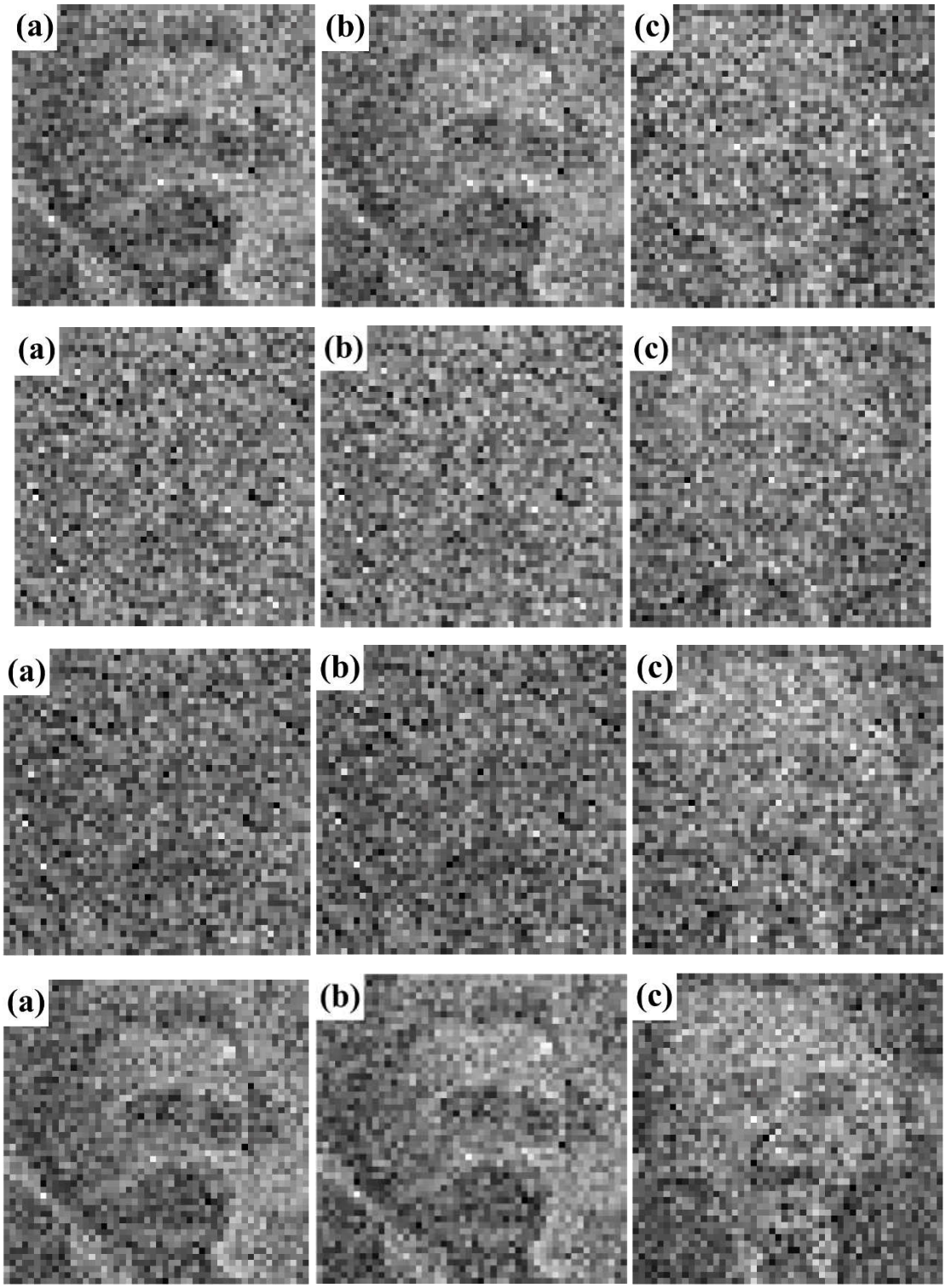

Figure 23 - Recovered images from the two channels and the secret image for different percentages of data being revealed. Cover image (channel one) (a), secret image embedded in cover image (channel two) (b), and secret image (c). Percentages of data disclosure from top to bottom for random matrices and buckets respectively are: 100-96, 50-100, 60-100, 100-100.

CHAPTER 5

CONCLUSIONS

5. Conclusions and future works

Multiple layers of information encryption are introduced based on computational single pixel imaging on top of one another to provide high level of information security. For the first layer, we made use of two channels (extendable to multiple channels) corresponding to the data coming from 3D CGI each with a different angle of view. We showed, by the NRMS metric, that distributing information among different channels increases the security as it necessitates attacks on all channels. We showed that this first layer of security is breakable by more than 40-50 percent of matrices (secret keys) being revealed. We further enhanced the robustness of CGI-based information encryption schemes by uniting different channels using another private key associated to the order with which bucket data from channels are put in a sequence. Unauthorized recovery of information becomes computationally heavy and time consuming since the attacker needs to run CGI algorithm (trying random matrices) for large fraction of all probable permutations of bucket data. Besides the superior performance in securing the information, it is shown that the importance of using right bucket sequence for retrieving image is more critical than that of random matrices. If considered independent from the security provided in the first layer, it is demonstrated that by having access to more than 50 percent of correct bucket data sequence, the recovery is possible.

Finally, CGI-based steganography is introduced and an ultimate security level is achieved. We designed a scheme where using partially incorrect sequence of bucket data (in presence of

correct random matrices obtained) gives the attacker the same fooling image from both channels. The idea is feasible since in the best case, attackers recover the cover image unless they get access to almost all keys related to random matrices, bucket data sequence, and the way the secret image is embedded in the cover image. This entails that a successful retrieval of information requires more than 96 percent of bucket values of the second layer to be disclosed along with almost the same percentage of random matrices of the first layer.

In future works we propose to use digital data instead of images and study the encryption based on them.

References

[1] A. Alfalou and A. Mansour, Double random phase encryption scheme tomultiplex and simultaneous encode multiple images, Applied Optics 48, 5933 (2009).

[2] G. Unnikrishnan, J. Joseph, and K. Singh, Optical encryption by double random phase encoding in the fractional Fourier domain, Optics Letters 25, 887 (2000).

[3] G. Situ and J. Zhang, Double random-phase encoding in the Fresnel domain, Optics Letters 29, 1584 (2004).

[4] Z. Liu, H. Chen, T. Liu, P. Li, J. Dai, X. Sun, and Sh. Liu, Journal of Optics, Double-image encryption based on the affine transform and the gyrator transform, 12, 035407 (2010).

[5] T. Nomura and B. Javidi, Optical encryption using a joint transform correlator architecture, Optical Engineering 39, 2031 (2000).

[6] Y. Zhang and B. Wang, Optical image encryption based on interference, Optics Letters 33, 2443 (2008).

[7] B. Javidi and T. Nomura, Securing information by use of digital holography, Optics Letters 25, 28 (2000).

[8] W. Chen, X. Chen, and C. Sheppard, Optical image encryption based on diffractive imaging, Optics Letters 35, 3817 (2010).

[9] B. Javidi and T. Nomura, Polarization encoding for optical security systems, Optical Engineering 39, 2439 (2000).

[10] Sh. Liu, Ch. Guo, and J. T. Sheridan, A review of optical image encryption techniques, Optics & Laser Technology 57, 327 (2014).

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Reviews of Modern Physics 74, 145 (2002).

[12] B. Javidi, ed., Optical and Digital Techniques for Information Security (Springer Verlag, New York, 2005).

[13] A. Belazi, A. A. Abd El-Latif, and S. Belghith, A novel image encryption scheme based on substitution-permutation network and chaos, Signal Process. 128 155 (2016).

[14] H. J. Liu and A. Kadir, Asymmetric color image encryption scheme using 2D discrete-time map, Signal Processing 113 104 (2015).

[15] W. Zhang, H. Yu, Y.L. Zhao, and Z.L. Zhu, Image encryption based on threedimensional bit matrix permutation, Signal Processing textbf118 36 (2016).

[16] Y. C. Zhou, L. Bao, and C. L. Philip Chen, A new 1D chaotic system for image encryption, Signal Processing 97 172 (2014).

[17] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, A novel color image encryption algorithm based on spatial permutation and quantum chaotic map, Nonlinear Dynamics 81 511 (2015).

[18] M. Kumar, A. Iqbal, and P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography, Signal Processing 125 187 (2016).

[19] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Optics & Lasers Engineering 73 53 (2015).

[20] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, A novel chaosbased image encryption using DNA sequence operation and secure hash algorithm SHA-2, Nonlinear Dynamics 83 1123 (2016).

[21] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata, Optics & Laser Engineering 71 33 (2015).

[22] A. Souyah and K. M. Faraoun, Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata, Nonlinear Dynamics 84 715 (2016).

[23] P. Ping, F. Xu, and Z. J. Wang, Image encryption based on non-affine and balanced cellular automata, Signal Processing 105 419 (2014).

[24] X. L. Chai, An image encryption algorithm based on bit level Brownian motion and new chaotic systems, Multimedia Tools and Applications 76 1159 (2017).

[25] X. Y. Wang and D. H. Xu, A novel image encryption scheme based on Brownian motion and PWLCM chaotic system, Nonlinear Dynamics 75 345 (2014).

[26] G. D. Ye, A block image encryption algorithm based on wave transmission and chaotic systems, Nonlinear Dynamics 75 417 (2014).

[27] X. F. Liao, S. Y. Lai, and Q. Zhou, A novel image encryption algorithm

based on selfadaptive wave transmission, Signal Processing 90 2714 (2010).

[28] Y. Wu, Y. C. Zhou, P. N. Joseph, and A. Sos, Design of image cipher using latin squares, Information Sciences 264 317 (2014).

[29] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Prez-Cabr, M. S. Milln, N. K. Nishchal, R. Torroba, J. F.Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse,T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, and A. Markman, Roadmap on optical security, Journal of Optics 18, 083001 (2016).

[30] J. H. Shapiro and R. W. Boyd, The physics of ghost imaging, Quantum Information Processing 11, 949 (2012).

[31] Y. Bromberg, O. Katz, and Y. Silberberg, Ghost imaging with a single detector, Physical Review A 79, 053840 (2009).

[32] G. Scarcelli and V. Berardi, and Y. Shih, Can Two-Photon Correlation of Chaotic Light Be Considered as Correlation of Intensity Fluctuations?, Physical Review Letters 96, 063602 (2006).

[33] J. H. Shapiro, Computational ghost imaging, Physical Review A 78, 061802R (2008).

[34] Y. Wang, J. Suo, J. Fan, and Q. Dai, Hyperspectral Computational Ghost Imaging via Temporal Multiplexing, IEEE Photonics Technology Letters 28, 288 (2016).

[35] T. Mao, Q. Chen, W. He, Y. Zou, H. Dai, and G. Gu, Speckle-Shifting Ghost Imaging, IEEE Photonics Journal 8, 6900810 (2016).

[36] M. Lyu, W. Wang, H. Wang, H. Wang, G. Li, N. Chen, and G. Situ, Deep-learning-based ghost imaging, Scientific Reports 7, 17865 (2017).

[37] J. Tang, Y. Tang, K. He, L. Lu, D. Zhang, M. Cheng, L. Deng, D. Liu, and M. Zhang, Computational Temporal Ghost Imaging Using IntensityOnly Detection Over a Single Optical Fiber, IEEE Photonics Journal 10, 7101809 (2018).

[38] X. Wang and Z. Lin, Microwave Surveillance Based on Ghost Imaging and Distributed Antennas, IEEE Antennas and Wireless Propagation Letters 15, 1831 (2016).

[39] B. Sun, M. P. Edgar, R. Bowman, L. E. Vittert, S. Welsh, A. Bowman, and M. J. Padgett, 3D computational imaging with single-pixel detectors, Science 340, 844 (2013).

[40] P. Clemente, V. Durn, V. Torres-Company, E. Tajahuerce, and J. Lancis, Optical encryption based on computational ghost imaging, Optics Letters 35, 2391 (2010).

[41] B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, Normalized ghost imaging, Optics Express 20, 16892 (2012).

[42] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, Gray-scale and color optical encryption based on computational ghost imaging, Applied Physics Letters 101, 101108 (2012).

[43] J. Zang, Zh. Xie, and Y. Zhang, Optical image encryption with spatially incoherent illumination, Optics Letters 38, 1289 (2013).

[44] M. Zafari, R. kheradmand, and S. Ahmadi-Kandjani, Optical encryption with selective computational ghost imaging, Journal of Optics 16, 105405 (2014).

[45] M. Tanha, S. Ahmadi-Kandjani, R. Kheradmand, and H. Ghanbari, Computational fluorescence ghost imaging, The European Physical Journal D 16, 44 (2013).

[46] H. Ghanbari-Ghalehjoughi, S. Ahmadi-Kandjani, and M. Eslami, High quality computational ghost imaging using multi-fluorescent screen, Journal of Optical Society of America A 32, 323 (2015).

[47] W. Chen and X. Chen, Marked ghost imaging, Applied Physics Letters 104, 251109 (2014).

[48] L. Wang, Sh. Zhao, W. Cheng, L. Gong, and H. Chen, Optical image hiding based on computational ghost imaging, Optics Communications 366, 314 (2016).

[49] S. Liansheng, Ch. Yin, T. Ailing, and A. K. Asundi, An optical watermarking scheme with two-layer framework based on computational ghost imaging, Optics and Lasers in Engineering 107, 38 (2018).

[50] Sh. Jiao, Ch. Zhou, Y. Shi, W. Zou, and X. Li, Review on optical image hiding and watermarking techniques, Optics and Laser Technology 109, 370 (2019).

[51] Y. S. Zhang, L. Y. Zhang, J. T. Zhou, L. C. Liu, F. Chen, and X. He, A review of compressive sensing in information security field, IEEE Access 5, 2507 (2016).

[52] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals, IEEE Transactions on Signal Processing 62, 196 (2014).

[53] Y. S. Zhang, J. T. Zhou, F. Chen, L. Y. Zhang, W. Kwok-Wo, X. He, and D. Xiao, Embedding cryptographic features in compressive sensing, Neurocomputing 205, 472 (2016).

[54] N. R. Zhou, H. L. Li, D. Wang, S. M. Pan, and Z. H. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Optics Communications 343, 10 (2015).

[55] X. J. Tong, M. Zhang, Z. Wang, and J. Ma, A joint color image encryption and compression scheme based on hyperchaotic system, Nonlinear Dynamics 84, 2333 (2016).

[56] H. Liu, D. Xiao, R. Zhang, Y. S. Zhang, and S. Bai, Robust and hierarchical watermarking of encrypted images based on compressive sensing, Signal Processing: Image Communication 45, 41 (2016).

[57] N. R. Zhou, J. P. Yang, C. F. Tan, S. M. Pan, and Z. H. Zhou, Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform, Optics Communications 354, 112 (2015).

[58] R. Huang, K. H. Rhee, and S. Uchida, A parallel image encryption method based on compressive sensing, Multimedia Tools and Applications 72, 71 (2014).

[59] M. A. Qureshi and M. Deriche, A new wavelet based efficient image compression algorithm using compressive sensing, Multimedia Tools and Applications 75, 6737 (2016).

[60] P. Lu, Z. Y. Xu, X. Lu, and X. Y. Liu, Digital image information encryption based on compressive sensing and double random-phase encoding technique, Optik 124 2514 (2013).

[61] P. Refregier and B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Optics Letters 20, 767 (1995).

[62] N. Takai and Y. Mifune, Digital watermarking by a holographic technique, Applied Optics 41, 865 (2002).

[63] M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, and X. F. Meng, Multiple image encryption and watermarking by random phase matching, Optics Communications 247, 29 (2005).

[64] Y. Shi, G. Situ, and J. Zhang, Multiple-image hiding in the Fresnel domain, Optics Letters 32, 1914 (2007).

[65] X. Shi and D. Zhao, Image hiding in Fourier domain by use of joint transform correlator architecture and holographic technique, Applied Optics 50, 766 (2011).

[66] Baris I. Erkmen and Jeffrey H. Shapiro, Ghost imaging: from quantum to classical to computational, Advances in Optics and Photonics, 2, 405–450 (2010).

[66] Yoann Altmann, Stephen McLaughlin, Miles J. Padgett, Vivek K Goyal, Alfred O. Hero, Daniele Faccio, Quantum-inspired computational imaging, Science, 361, 6403 (2018).