International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *23 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *25 October 2023*

Steganography using AES and Edge Image

Jannah Raad Taher [1], Sundus Q. Habeeb[2], Safaa D. Al-Khafaji[3]
[1]Jabir ibn Hayyan Medical University, Najaf, Iraq
[2]Faculty of Medicine, Jabir ibn Hayyan Medical University, Najaf, Iraq
[3]Department of Computer Sciences, College of Education for Girls, Kufa University, Najaf, Iraq
Corresponding Author:
Jannah Raad Taher
Jabir ibn Hayyan Medical University.
Najaf, Iraq
E-mail: Jannah.raad@jmu.edu.iq

Abstract: Steganography is the art of hiding messages in an image. This is a great way to send a secret message without drawing attention to it. Many technologies have been developed to ensure data security, and cryptography is considered one of the most important sciences used since the dawn of humanity. Using this proposed technique, we take the input text(128-bit) with key(128-bit), encrypt it using AES technology, and then hide out text(128-bit) inside the edges of the image free size. This is done by extracting the edges of the image and combining them with the ciphertext to make them disappear completely. Text data security is a good thing with this proposed new technology. It is also easy to extract text from the edges of the image and re-decode it. The resulting image is the same as the selected image, clear with raised edges, with text disappearing within the edges of the image indistinguishable from the naked eye. Therefore, this proposed method is considered the safest in hiding data inside the image.

Keywords: Steganography, Edge Detection, AES Algorithm, Hidden Text, Edge Image.

1. Introduction

We employ cryptography to protect sensitive information because it is one of the fundamental requirements for completing any task requiring high levels of security. Abbas.C and ETL Used an algorithm (1D SHA-2) in conjunction with a composite forward transformation, to describe a technique for password-protected digital image encryption. Used the coupled symmetry of the Fourier transform's composite image ingredient, they created a locative mask from the frequency domain. Following that, they xored that mask with the bit stream of the main picture. The asymmetric Boolean operations known as an exclusive OR, or XOR, returns 1 if both binary pixels are one, 0 if either is zero, or 0 otherwise. This can be verified with just the argument (Pixel1, Pixel2, 2). Lastly, they used confusion depended on a reference mask offset of the pixels in the code. They examined the method's security and performance facets, which demonstrated this approach is active and secured from a perspective of the cryptographic. Such as algorithm ability to force a continued tone payload—the steganography term to map to a balance bit distribution series is one of its benefits. Because steganography and watermarking are possibly to have a balance perception effected on the cover of the picture when implanted, they require this bit balance [1].

Ahmad.A and ETL proposed used encryption. In applications using cryptography, the data being transferred is first encrypted in the source device using an encryption key before being forwarded to the destination device. With their approach, the hacker would not has access to the encryption keys needed to decrypt the main data, making it impossible for the hacker to manipulate the session. They employed private key encryption as their technique. Their approach is known as text-to-image encryption (TTIE) [2]. Ahmad.A and ETL the internet has reportedly been used for a variety of online activities. Data transmission over the Internet can be made secure by using encryption. They suggested a text to image encryption (TTIE) technique as a new algorithm for security networks in earlier work. They examine the TTIE large-scale aggregation efficiency in this study [3]. Used both full coding and selective coding strategies, Majid.K. and Tariq.S. presented provides a validation of picture coding in the spatial, frequency, and hybrid domains [4]. Abusukhon.A and ETL The TTIE algorithm has been examined on a single machine when a sizable dataset is employed, as suggested. The uptime was very high. To resolve this issue, To look into reducing coding time, they suggested the distributed TTIE (DTTIE) algorithm. In DTTIE, the server is in charge of evenly distributing a sizable amount of data (5.77 GB) among a number of nodes [5]. Kundankumar.RS and ETL, and They used AES to implement text and image encryption and decryption as suggested. The Code Composer Studio program was used in conjunction with straightforward C language code to synthesis and simulate 128-bit text entries for text encoding on a TMS320C6713 DSP processor. The SDK for the Java Application Platform was used to create and simulate Java code to encrypt the photos. For encoding images, CBC mode is typically used in conjunction with PKCS 5 padding [6].

Heidilyn V. Gamido and ETL, As suggested, the Advanced Encoder Standard was changed to handle its increased processing needs as a result of the mixcolumns transformation's poor encoding speed and complicated arithmetic operations. Bit permutations, which are simple to use and do not require intricate mathematical computations, have replaced the mixcolumns conversion in modified AES. According to the study's findings, the updated AES algorithm was more efficient since it encrypts data more quickly and uses less CPU power. The new AES algorithm also produced a stronger avalanche effect, which enhanced the algorithm's performance [7]. Shanthakumari, R., and Malliga, S. The suggested outlines the application of a new steganography technique that extracts and embeds private information used the Least - Significant - Bit -Grouping (LSBG) mechanism and the International Information Encryption Standard (IDEA) algorithm. The outcome demonstrates enhanced data embedding capabilities and decreased data security concerns through the efficient application of this innovative approach, which exhibits the great accomplishment of combinatorial implementation of steganography and encryption technology. In order to successfully use steganography in a data security system, IDEA and LSBG possess several essential properties like information secrecy, verification, integrity, robustness and capability. Several specialized metrics, such as root means square error, mean square error, and peak signal-to-noise ratio structural similarity index matrix for picture quality analysis, can be used to assess the efficiency and qualities of the stego image. According to the findings, the suggested technology performs better than the existing approaches and addresses the issue of the security data in the transmission data and storage systems for cloud compute services [8].

TTIE algorithm has a new security level proposed by Ahmad.A and ETL, and it is demonstrated how the Diffie-Hellman method is used to exchange the TTIE generated the encryption key algorithm with the other part. As a result, this work examined and evaluated the proposed algorithm and suggested a modified TTIE technique named Diffie- Hellman Text-to-Image Encryped Algorithm (DHTTIE) [9]. Yasser.M, proposed prototype was tested on the dataset utilizing the provided programming using 20 useable photos and text messages (normal data). Simulated data transmission distance and normal data volume were used to analyze security performance utilizing the local server. A number of attacks were launched throughout the simulation test utilizing well-known attack methods including Stego Picture Quality Monitoring. The experiment's findings revealed that around 85% of the attack trys failed to capture the stego. 95 percent of attacks fail to re-planning useful data points from jumbled data. The outcomes show how effective the suggested security techniques are at protecting Internet data transfer. To maintain a high level of security for data transmission over the Internet, this work effectively integrated steganography and random mapping methods [10].

Vishruti.K and ETL proposed the use of biometric authentication to secure photographs on a cloud platform. The many processes involved in secure image and biometric authentication uploading and access described, and all procedures are merged at the conclusion as a case study to show the overall process and emphasize the ways that are best in terms of results and compatibility. With the help of the hybrid SHA/Blowfish method for picture encryption, and the classic discrete wavelet transform method for image compression, this methodology presented the concept of image authentication in the only simple two steps. Following that, the user can retrieve this image whenever they want by requesting it from a cloud database. Images, biometric kinds, rics, safe data, and encryption techniques have all been covered in detail [11]. An image coded system is presented that was proposed by Roayat.I.A and ETL. The plan is divided into two phases. In order to decrease the amplitude of the encryption data and render that data visually inaccessible to unauthorized employees, the patient data (such as name, age, etc.) was first concealed in the patient's medical images (such as an MRI, X-ray, etc.). in their behalf. Second, a brand-new multi-chaos mapping technology was used to code the patient's medical image. The novel multi-chaos map is a Henon, Sin, and Tenmapsp (HST) fusion of pseudo-random sequences with more chaotic features, but DNA coding increases computational speed and offers huge data transfer capacity. The findings demonstrate that their method can withstand statistical and differential attacks, has a large key space, low correlation, key-dependent pixel-value substitution, and an excellent peak signal-to-noise ratio [12]. A region of interest (ROI) depended on eclectic image coding was propose by Kiran and Colleagues. The ROI and background (ROB) area were initially divided using segmentation of the active contour image. The diffusion and permutation methods were then put into practice using the Hilbert curve and the Skew Tent map. In order to lessen the similarity between the internal neighboring pixels, the ROI portion was moved in accordance with the Hilbert scan pattern. Then, depended on a predetermined threshold value from the Skew Tent map, the pixels in the alternating ROI section are XOR pixels with randomly numbers. After that, encrypted pictures are created by combining the encrypted ROI and ROB blocks [13]. Summarized recent developments in environmentally friendly and secure printing, Yun Ma and Coworkers proposed a number of smart materials that react to numerous external stimuli, such as water, light, heat, metal ions, and ph. In the quickly expanding research field, they also talked about present difficulties and potential directions [14].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *23 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *25 October 2023*

2. Methodologies

In this proposed study, we take the input text and encrypt it using AES to produce ciphertext, and then we extract the edges of the selected image and hide the ciphertext in their place. As shown in the figure 1 below

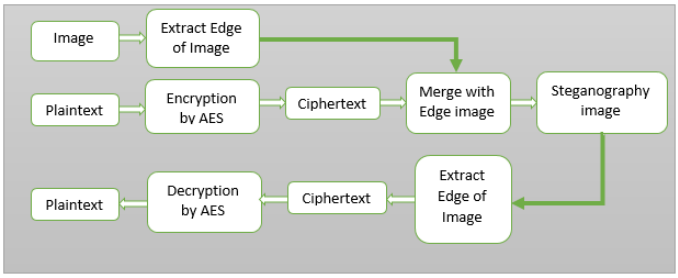
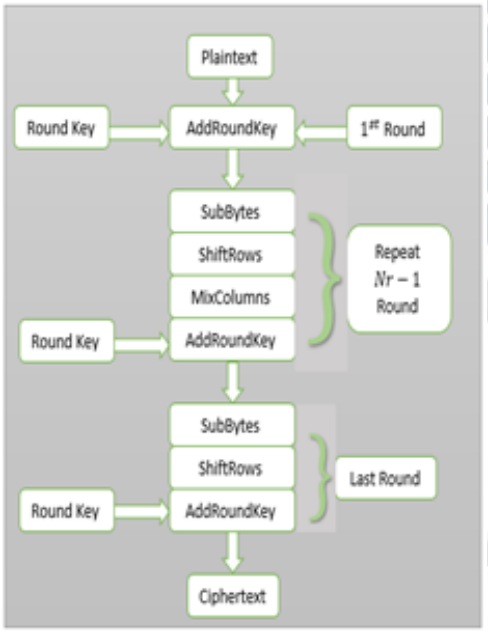


Figure 1 : The Method of Work

2.1 AES Encryption and Decryption

As seen in figure 2 below, this encryption technique starts with the plaintext text to be encrypted (plaintext) and adds a key to it using the Addroundkey operation before working on it using SubBytes, Shiftrows, Mixcolumns, and other operations.



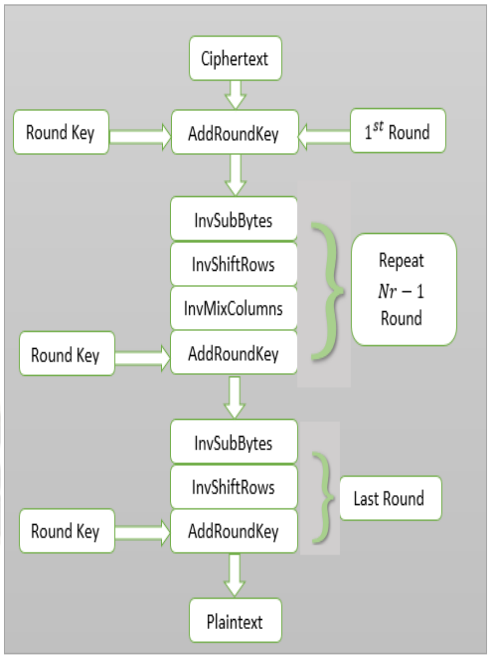


Figure 2 : AES Encryption and Decryption

2.1.1 AES Rounds

For the AES algorithm, the input, output block and the State length is 128 bits . This is symbolized by Nb = 4, that corresponds to the State's 32-bit word count (number of column). the Cipher Key length, K, for the AES algorithm are 128, 192, or 256 bits. Nk represents the block's key length and has a value of 4, 6, or 8. This value represents how many 32-bit words (columns) there are in the Cipher Key.

The rounds number must be complete during the AES algorithm's execution based on the size of the key. The rounds number are denoted by Nr. For both its cipher text and the inverse of the cipher text, the AES algorithm used the round function. The oriented of the four byte changes that make up this function are as follows: A) By replacing bytes using a substitution tables (S-box); B) the rows of the State array are Shifting by various offsets; C) combining the values for each State in the array column; and D) a Round Key is adding to the State. The number of round keys that the key expansion algorithm generates is always more than the actual number of the rounds by adding one another round in the process. That, can be written the equation as follows:-

$$Number\ of\ round\ keys = Nr + 1 \qquad (1)$$

$$We\ refer\ to\ the\ round\ keys\ as\ K_0.K_1.K_2 \ldots\ldots\ldots\ldots K_{Nr}$$

2.1.2 The Method

The AES method transforms the input (block size Nb, commonly referred to as plaintext) into a 4 x 4 matrix known as state. To determine the output state, four transformations—

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 23 August 2023 **Revised:** 10 October 2023 **Accepted:** 25 October 2023*

Adding a Round Key, Sub Bytes, Shifts Rows, and Mixed Columns—perform different operations on the state (at the final cipher text). All operations, with the exception of Adding a Round Key, are reversible. Method(a) invMethod = a (2) A variable is returned if Adding a Round Key performs operations on it twice.

2.1.3 Modification in AES

The following mathematical procedures are necessary to comprehend in order to carry out all the transformations mentioned above

a. Routine Adding a Round Key

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

=

$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

Adding a round keys and a piece of an enlarged keys into plaintext using the Adding a Round Key function is as easy as using XOR.

b. the Sub Bytes

The SBOX for AES is subbyte. AES is a non-linear cryptographic system because it proceed a non-linear substitution to the GF(28) fields and acts on each byte in the state. Every value of b' that is derived from a unique value of b is required for the function to be invertible. SubBytes can also be implemented with a look-up table. The SubByte method adds byte b's inverse to 0xC6 after performing an affine transformation on it.

c. ShiftRows

On certain the state's rows, ShiftRows executes. It offers spread across the entire AES algorithm. There is no modification to the first row. With the left most byte wrapping around, at the second row is moved to the left only one byte. Two bytes are moving to the left in the third row, three bytes are moving to the left in the fourth row with the proper wrapping to the right. The amount of shifts for each row varies depending on the size of the key in the example given below for AES-128.

d. MixColumns

On certain state columns, MixColumns operates. Diffusion is provided across the entire AES algorithm. The columns are multiplied by a(x) modulo $x_4 + 1$, $where\ a(x) = 03x_3 + 01x_2 + 01x + 02x$, and the rows are treated as polynomials over GF(28). REMEMBER: x4+1 is essentially prime to a. (x). An equation in a matrix can be used to represent this:

$$\begin{bmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

This can be transformed into an equation system that can be solved using the addition and multiplication principles outlined in section 2 of this article. The equation: can be used to describe InvMixColumns.

$$\begin{bmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Loops The AES algorithm through certain parts (N) times, as seen in figure 2 above. In order to give the algorithm initial and final randomization, the AddRoundKey is executed at the start and end of the cipher. Without this operation, it would be simple for anyone to deduce the initial or last part of the cipher, making it irrelevant to the security of the cipher. The final round of the cipher is totally various from the other rounds in order to make the encryption and decryption processes more similar. Implementations of hardware and software become less complex as a result.

2.2 Steganography Image

Choose the image in which you want to hide the text, regardless of its size (R, C), then extract its edges using canny edge and place it in a one-dimensional matrix, then replace it with the ciphertext and then reposition it with the two-dimensional matrix and then merging it with the original image are the steps of the proposed process. We repeat the above procedures in reverse if we want to recover the ciphertext to decrypt it. As shown in the figure 3 below:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *23 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *25 October 2023*

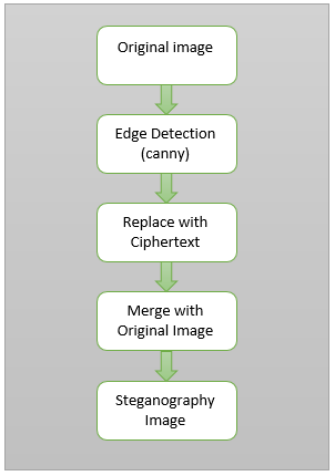


Figure 3: Steganography Image

3. Results

The proposed method is based on hiding the text inside the selected image after using AES to encrypt it. The results are displayed using several images and as shown in the figuers below Figure 4 (cameraman) image, Figure 5 (peppers) image, Figure 6 (coins) image, Figure 7 (eight) image. As shown in paragraph (a) the original image, (b) extracting edges, and (c) the information is hidden inside the image (steganography image).

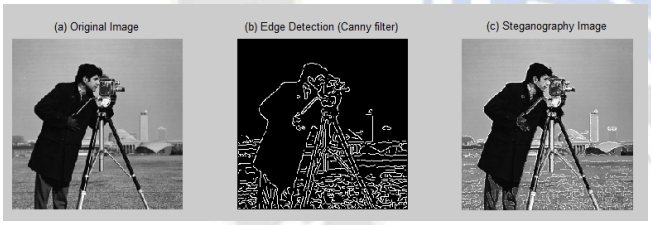


Figure 4: (cameraman) image

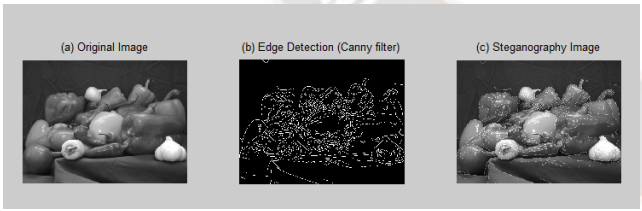


Figure 5: (peppers) image

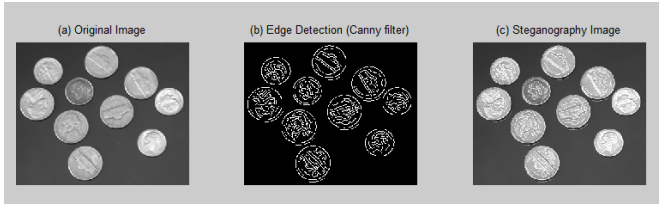


Figure 6: (coins) image

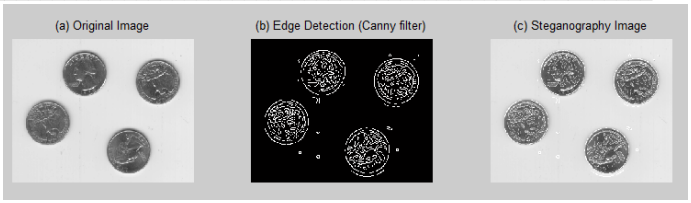


Figure 7: (eight) image

4. Conclusion and Further Work

This method is considered the first in terms of hiding information within the edges of the image. The following is the conclusion:

1. Choose several encryption techniques if you discover the best one.

2. Choose a color image instead of a grayscale image to hide the encrypted information in one of its layers.

3. The proposed system can be expanded to include video systems to hide information in a long message.

4. Hide an image within the edges of another image, or encrypt a group of images within the edges of the selected image.

5. Hide a file inside the edges of the image

6. Improving the image if the resulting image after masking is unclear, even if the percentage of this possibility is very small because our system works only on the edges of the image to highlight it more clearly.

References

[1] Cheddad, Abbas, et al. "A hash-based image encryption algorithm." *Optics communications* 283.6 (2010): 879-893.

[2] Abusukhon, Ahmad, Mohamad Talib, and Issa Ottoum. "Secure network communication based on text-to-image encryption." *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 1.4 (2012): 263-271.

[3] Abusukhon, Ahmad, Mohammad Talib, and Maher A. Nabulsi. "Analyzing the efficiency of Text-to-Image encryption algorithm." *International Journal of Advanced Computer Science and Applications* 3.11 (2012).

[4] Khan, Majid, and Tariq Shah. "A literature review on image encryption techniques." *3D Research* 5 (2014): 1-25.

[5] Ahmad, Abusukhon, Talib Mohammad, and Hani Mahmoud Almimi. "Distributed text-to-image encryption algorithm." *International Journal of Computer Applications* 106.1 (2014).

[6] Saraf, Kundankumar Rameshwar, Vishal Prakash Jagtap, and Amit Kumar Mishra. "Text and image encryption decryption using advanced encryption standard." *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 3.3 (2014): 118-126.

[7] Gamido, Heidilyn V., Ariel M. Sison, and Ruji P. Medina. "Modified AES for text and image encryption." *Indonesian Journal of Electrical Engineering and Computer Science* 11.3 (2018): 942-948.

[8] Shanthakumari, R., and S. Malliga. "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment." *Sādhanā* 44 (2019): 1-12.

[9] Abusukhon, Ahmad, et al. "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm." *Journal of Discrete Mathematical Sciences and Cryptography* 22.1 (2019): 65-81.

[10] Al-Sharo, Yasser Mohammad. "Images Steganography Approach Supporting Chaotic Map Technique for the Security of Online Transfer." *International Journal of Advanced Computer Science and Applications* 10.4 (2019).

[11] Kakkad, Vishruti, Meshwa Patel, and Manan Shah. "Biometric authentication and image encryption for image security in cloud framework." *Multiscale and Multidisciplinary Modeling, Experiments and Design* 2 (2019): 233-248.

[12] Abdelfattah, Roayat Ismail, Hager Mohamed, and Mohamed E. Nasr. "Secure image encryption scheme based on DNA and new multi chaotic map." *Journal of Physics: Conference Series*. Vol. 1447. No. 1. IOP Publishing, 2020.

[13] Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and computation of encryption technique to enhance security of medical images." *IOP Conference Series: Materials Science and Engineering*. Vol. 925. No. 1. IOP Publishing, 2020.

[14] Ma, Yun, et al. "Stimuli-responsive photofunctional materials for green and security printing." *InfoMat* 3.1 (2021): 82-100.