International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.18, June 2025

A Functional Android Application Implementing Universal Share based Multi Secret Sharing Scheme with Two-in-one Decoding Options

Dipak K. Rabari
Assistant Professor
Department of Electronics & Communication
Faculty of Technology,
Dharmsinh Desai University, Nadiad, INDIA.

Yogesh K. Meghrajani,
Senior Member, IEEE
Associate Professor
Department of Electronics & Communication
Faculty of Technology,
Dharmsinh Desai University, Nadiad, INDIA.

Laxmi S. Desai
Professor
Department of Mathematics
Faculty of Technology,
Dharmsinh Desai University, Nadiad, INDIA.

ABSTRACT

In the twenty-first century, Mobile phones are utilized for applications beyond communication; people are encouraged to use them for personal computing due to the fact that they are more affordable, lighter, and smaller than computers. In this paper, the development of mobile application is presented for secret sharing schemes that necessitate a computing device in order for the recipient to decrypt the data. To discover the secret image at the receiver, a computer is a necessary computation device. An executable Android application that features rotating random grids and dual decoding options for the universal share-based multi secret sharing scheme is developed. The application scenario includes both previewing and high-quality lossless recovery of multiple secrets in the proposed scheme. The presented Android application is useful in the recovery of high-quality lossless secret images. The usability of this proposed scheme is assessed and comprehend the underlying security model.

General Terms

Visual secret sharing, Android application development

Keywords

Universal share, Multi-secret sharing scheme, Two-in-one decoding scheme, Random Grid.

1. INTRODUCTION

Due to the increasing use of operating system-focused applications (Android, iOS, etc.), mobile devices are becoming indispensable element of every person in recent years. Voice communication is the primary use of mobile devices. It is also used to store media files, including videos and pictures. Mobile phone applications have evolved for social and commercial purposes, despite their initial use for entertainment and gaming. Nonetheless, the need to be in constant communication drives developers to generate various types of commercial and social mobile applications. Compare to phone-size devices, tablets can be used to execute applications comfortably. Mobile health applications [3] and industrial applications [2] are examples of recent Android application development research. Additionally, the creation of Android applications presents a likelihood for additional study and advancement to raise the caliber of software for user-friendliness.

Google Android is the provider behind the Android mobile operating system. The main purpose of Android is for mobile devices, including tablets and smartphones. Android offers an application framework in addition to using the Linux kernel. The application programmable interfaces (APIs) and tools needed to start creating Android applications with Java as the programming language are provided by the Android software development kit (SDK). The Google Play App Store and Android Market are two online stores where users can access the developed mobile Android apps. Because Android offers a customized operating system for high-tech devices, it is far more dependable and user-friendly than other similar technology companies.

Naor and Shamir [7] proposed visual cryptography (VC), a prototype for secret sharing schemes (SSS) that enables the decoding of hidden images without the need for a computer or cryptographic expertise. In particular, a secret image is split up into n random noise-like shares in a k-out-of-n visual SSS. It is possible to print these n shares onto transparencies and give them to n participants. A secret image can be unveiled without the requirement of computational resources by stacking any k or more share transparencies.

However, stacking fewer than k shares does not allow for the recovery of any information about the secret image. The disadvantages of this scheme include the need for a code-book, poor contrast, pixel alignment and pixel expansion in the recovered image. In order to encode the secret image into noise-like random shares, Kafri and Keren [4] proposed a random grid-based (RG) 2-out-of-2 visual SSS. The principal advantage of using this RG-based approach is that, it eliminates the need for code-book and pixel expansion in the generated shares. But their scheme also has poor contrast and pixel alignment issues. Although RG-based SSS [4] is not suitable for such scheme where it is necessary to create n shares (n $>$ 2). Amongst these n shares, k shares must disclose the secret in a threshold (k, n) SSS; shares below k shares are not allowed to divulge any information. By adding minimal computation at the receiver, Boolean-based SSS are used to address problems such as pixel alignment and low contrast of the disclosed secret image. An XOR operation is employed to mathematically describe the operation for the computation on images of the VC system. To decode the secret image at the receiver, the scheme must execute XOR operations. Lossless reconstruction of the original secret image at the recipient is the primary benefit of Boolean-based secret sharing schemes. Furthermore, information processing with quantum secret sharing techniques is being adopted by current research trends [9].

Subsequently, rather than sharing a single secret image, Multi Secret Sharing Schemes (MSS), which efficiently utilize the available channel capacity, are used. Multi-secret sharing (MSS) schemes have been proposed by numerous researchers [10][1]. In recent years, the universal share approach has been used to share multiple secrets using common share. To share n secret images, n shares are required, along with a universal share that is a necessary common share. All n+1 shares are required in order to recover all n secret images. Remarkably, all n+1 shares are not needed to retrieve a single secret image, in contrast to traditional multi-secret sharing (MSS) schemes. A system based on universal share helps the chief authority of an organization increase the level of secrecy because the authority has the universal share that needs to be used to decrypt the secrets. Meghrajani and Mazumdar [6] presented a universal share-based multi secret visual secret sharing scheme (MSVSS) based on Boolean operations. This scheme offers lossless reconstruction with less computational complexity. Two distinct decoding methods are offered by a different class of VSS schemes. Through share stacking and computational processes, these schemes enable the disclosure of the hidden image. Likewise, each share is used as a two-in-one information carrier in two-in-one decoding secret sharing schemes. The user can physically stack any k received transparencies to get a low contrast black-and-white view of the secret image, even if the decoding computer system is momentarily unavailable. However, a much more comprehensive view of the secret image can be obtained by using the information hidden in the shares through simple computation once the decoding computer system is eventually available. The efficacy of two-in-one decoding SSS is demonstrated by recent schemes [5][13]. The share images in earlier systems were square-shaped, noise-like shadow images that could share a limited number of secret images, indicating a research gap. Consequently, secret sharing schemes based on circular shares have emerged [12]. In order to share multiple secrets, recent Boolean-based techniques [12] are proposed for two-in-one decoding methods. Recently, a new technique has been introduced [**?**] that uses universal share for two-in-one decoding multiple secrets with rotating shares. As the use of smart devices increases, an Android application for smartphones is created in this paper. Users of this device have access to mobile Internet, which allows them to connect to the device at any time and from any location in order to communicate with other users. The research objective of the propose scheme is to produce a workable Android application that implements the universal share-based two-in-one multi-image SSS [**?**] so that secret image sharing schemes can be used on mobile devices. The use of its security features and the necessity for such an application is demonstrated in this scheme . The remainder of the document is organized as follows: The methodology is explained in Section 2. System implementation and experimental results are detailed in Section 3. This paper is finally concluded in Section 4.

2. METHODOLOGY

Litterateurs have proposed the development of Android applications [11], [8]. As stated in [8], mobile phones are also utilized in applications to process the necessary image. In this study, an application scenario is established where the user is at one end of the communication channel and the dealer is at the other. The user is expected to compute received shares at the receiver, while the dealer is involved in the creation and transmission of the shares. For a universal share-based two-in-one decoding MSS scheme with rotating random grids, an Android smartphone application is created. Circular shares with a noise-like appearance are used to convey secret image information.

The proposed research includes developing an Android application that computes noise-like shares in order to retrieve the secret image, thereby implementing a universal share-based two-in-one decoding MSS scheme. According to Kafri and Keren's [4] RG algorithm, several secret images (G_1,G_2...G_n) are encrypted into n pie-shaped noise-like shares (S_1,S_2...S_n) and one universal share (S_0). The lossless recovery of the multi-secret images is achieved using the Boolean XOR operation. The scheme's efficiency is increased by using rotation of the shares for image information encoding and decoding. The process of creating encrypted shares involves manipulating every single pixel of the universal share image with each pixel of the n secret images.

The universal share is first created as a pie-shaped random share. Pixel-by-pixel manipulation between the universal share image and the n secret image is required to generate the remaining n pie shares. According to the encryption algorithm, these generated shares must be rotated at particular angles. The decryption algorithm demonstrates how these n shares and a universal share reconstruct secret images during decoding at the receiver. The user must provide two shares for the decryption of the secret image; first share out of the n shares and second share is universal share. By stacking the shares as specified in the decryption algorithm, the user can obtain a preview of the original secret information in the event when the computing device is unavailable. Little computation applied at the other end using a specially created Android application, this scheme provides the lossless retrieval of the secrets. The suggested scheme's decoding procedure uses the Boolean-based XOR operation, which reduces computational complexity. The threshold security is maintained in the suggested scheme because sharing secrets into n noise-like shares do not reveal any or all of the secret images from n-1 shares.

This scheme achieves effective network bandwidth utilization by using one share as a universal share for the computation in a mobile Android application for all n secrets. The proposed scheme effectively prevents hackers from revealing any partial information about the secret images, even if they manage to obtain access to any number of shares, unless they also have the universal share. Additionally, the secret can be recovered without loss due to XOR based computation technique. Moreover, the proposed technique is well

suited for the scenario where the strict authentication is mandatory requirement. The encryption and decryption algorithms in [**?**] are presented for ready reference .

2.1 Encryption algorithm

Input: *n* secret images (G_n)
Output: Universal share (S_0) and *n* shares (S_n)

(1) Generate the universal share as a first pie share (S_0) by assigning a random pixel value 0 or 1.
(2) Generate *n* random pie shares S_n using (S_0) and (G_n) by RG algorithm.
(3) Rotate pie share image S_1 clockwise by X degree, S_2 by 2X degree, and so on, whereas X=360/*n*.

2.2 Decryption algorithm

Input: Universal share (S_0) and *n* shares (S_n)
Output: *n* secret images (G_n)

(1) Rotate pie share image S_1 anticlockwise by X degree, S_2 by 2X degree, and so on, where X=360/*n*,
(2) Superimpose universal share S_0 with rotated share S_1 to reveal first secret image, similarly, stacking of S_2 with rotation reveals second secret, and so on.
(3) Perform XOR computation on universal share S_0 with rotated shares S_n to reveal lossless G_n secret images.

To decrypt the secret image, the dealer transmits the generated shares to the user via any preferred communication channel. The user applies a Boolean-based XOR operation to recover the high contrast secret image when a lightweight computing device, such as a desktop computer or even a laptop, is available. In this case, the device software performs the computation by analyzing the shares in accordance with the secret recovery algorithm of the SSS.
An Android application is developed that implements the universal share based two-in-one decoding MSS when the computing device is a mobile device. When computing devices like desktop computers or laptops are not easily accessible, this approach aims to perform the computation of shares on a decryption device, such as a mobile handset. During the secret recovery process, the dealer transmits a universal share along with another share from the set of n shares. The recipient's mobile device processes these two essential shares to reconstruct the image, which mirrors the original. The Android application that is installed on the user's mobile device examines the shares in order to recover the secret image.

3. SYSTEM IMPLEMENTATION AND EXPERIMENTAL RESULTS

3.1 Firmware and application

The mobile operating system (OS) products that control the market for developing mobile applications were created by a limited companies, including Microsoft, Apple, and Google. Every mobile operating system provides an SDK that includes an emulator, libraries, an integrated development environment (IDE), and other necessary tools. The program structure varies depending on the mobile operating system. When it is created for the PC environment, the programming language and development environment may be comparable. For instance, mobile applications for Windows and Symbian have essentially different code structures, but they can be programmed using the Microsoft Visual Studio environment and C++.

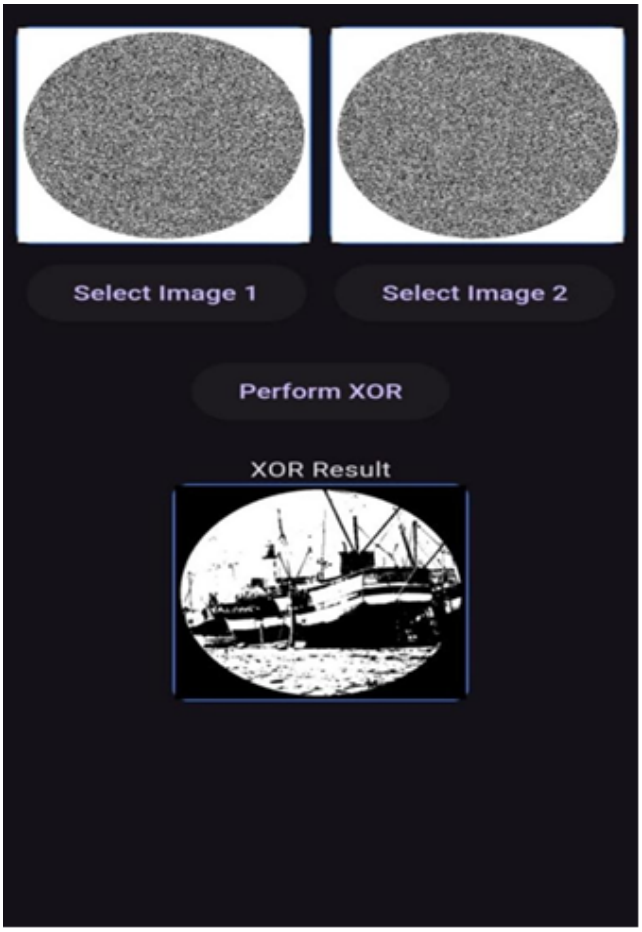

Fig. 1. Image 1 : Universal share image view on Android app; Image 2 : Share-1 image; XOR Result: The recovered secret image 1.

.

A mobile application is creted using the Android studio platform because of its adaptability and transparency. Android Studio is the official IDE for creating Android applications. IntelliJ IDEA software from JetBrains serves as its foundation. It is compatible with all major OS. Java is used to write the software code that implements this concept. In a similar vein, Android application development can be done with Google's main IDE, Eclipse Android Development Tools (ADT).
Microsoft Visual C# 2008 is used to create pie-shaped noise-like shares in order to implement the actual application scenario. As a dealer, a desktop computer with an 11th Gen Intel(R) Core (TM) i3-1115G4 CPU running at 3.00 GHz, 8 GB of RAM, and a 64-bit operating system is used to generate universal shares and n pie-shaped noisy shares. To recover the secret image, the mobile user is given the necessary universal share and n pie-shaped shares through a preferred communication channel. Installing the .apk file, which contains the image processing software code, is an essential requirement for the user. First, the pie-shaped share (S_1) and universal share (S_0) will be XORed to recover the first secret image. The remaining three secret images, (S_2), (S_3), and (S_4), will be recovered through the computation of universal share and rotated pie share. A Redmi Note smart phone, purchased from XIOMI

(China), serves as the image processing device. Version 13.0.10.0 (SKFINXM) of Android MIUI is integrated into this module.

3.2 Interface attributes

Various instances of the application must communicate with one another in order to perform the cryptographic calculations of the aforementioned secret sharing scheme. Numerous options, including WiFi, Bluetooth, mobile Internet, and others, can be used to implement smart phone communication effectively. Certain communication parameters, such as bandwidth, security, and display size, have an impact on the receiver's ability to decode the secret image.

The primary requirement for the application's is the confidentiality of the transmitted images in order to facilitate the development of SSS. To simplify comprehension, consider that the secure data is sent as a 4-digit numeric code. The probability of decoding the code is 10^4 (10,000) possible combinations. Although the secret data is sufficiently protected by these combinations, brute-force attacks which aim to test every possible combination can readily target it. For instance, if a single code attempt takes two seconds to execute, all codes can be tried in 5.55 hours. The actual code is likely to be retrieved before the estimated time. Alphanumeric codes can also be employed to lower the success rate of brute-force attacks. In general, it's possible to select well-known terms and recurring patterns as secret information. Because of this, it is usually advised to adopt an alphanumeric code with a minimum of six characters for everyday use. There are situations where the dealer shares partial secret information with the user in a single attempt, using a grayscale or color image. Attacks will be classified according to the resources they need in order to investigate the potential of the proposed scheme. It comprises the quantity and kind of cipher-grid needed for a specific technique, the number of computation steps to be completed, and the amount of storage needed to carry out the attack.

Since this scheme is a version of (2, 2)- VSS, decryption requires at least two shares. According to a brute-force attack, the 512 * 512 secret image in this developed application requires $(8 * 3)^{512*512}$ worst-case iterations. Furthermore, the computation device is needed to carry out specific computation steps to reconstruct the secret image. As a result, the developed Android application is secure. One crucial aspect of a communication medium is its data transfer efficiency. A wired network is the fastest data transfer medium. As an alternative to wired networks, limited-range wireless transfer methods like Wi-Fi and Bluetooth can also be used, offering a moderate speed. The distance between the transmitter and the receiver, electromagnetic interference, and the number of devices sharing the available bandwidth are some of the variables that affect the speed of any wireless transfer. Software hosted from a remote server can be operated on mobile devices.

As an alternative, it can make use of locally stored data. Bits per second are frequently used to express data transfer rates. Usually, the size of the data file is in bytes. Different image sizes and formats have an impact on how quickly secret images can be sent over communication channels.

3.3 Experimental results

The experiments are performed which evaluate the outcomes to ascertain the efficacy of mobile devices for visual cryptography. All experimental evaluation were conducted using 512 * 512 images. An Android application is created that displays various images in binary in order to test the efficacy of the suggested scheme. The calculated outcomes produced by Android Studio for four secret images shows the lossless recovery of multiple secret images.

Installing the .apk file on Redmi Note (Model: M2101K6P) mobile device allowed us to examine the usability of the developed Android application. A similar result was obtained when the XOR operation is performed on universal share and rotated share images to recover four secret images at receiver as shown in Figure 1 and Figure 3.

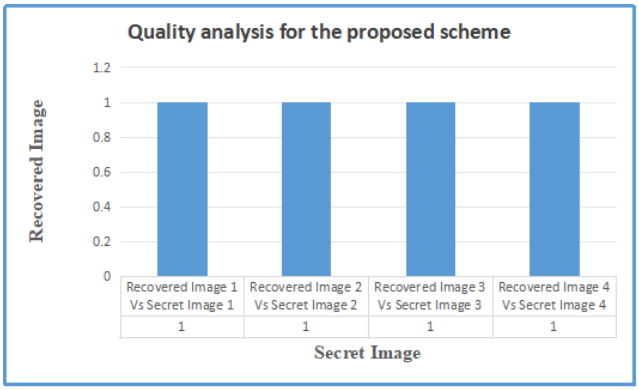

Fig. 2. Quality analysis

The experimental results for the implemented MSS for first binary secret out of four images is shown in Figure 1. By performing a logical XOR between two shares that were received from the dealer one as a universal share and the other as a circular share out of n shares the user will be able to reconstruct the first binary secret image out of four images. The bottom corner of Figure 1 reflects the lossless reconstruction of the first secret image. If the universal shares are not selected for calculation, the secret information remains hidden. Moreover, the other secret images can be recovered at receiver by performing computations on circular shares as per the decryption algorithm [**?**]. The experiment results depicted in Figure 3 shows the lossless recovery of the multi-secret images at receiver. The readability of the recovered image in comparison to the secret image is measured by the contrast. The contrast measurement indicates how apparent the reconstructed image is in comparison to the original. A precise reconstruction, which is due to the computation of shares at receiver attains the value of contrast as 1. The quality analysis of the proposed scheme with contrast measurement is depicted in Figure 2.

When a mobile device is used at the receiver, the suggested scheme supports the universal share-based scheme, in contrast to Rawat *et al.* [10]. Moreover, this scheme employs pie-shaped share images, which are used to share multi-secret images with shares rotated at a specific angle, in comparison to Rawat *et al.* [10]. Unlike Sridhar and Sudha, the implemented scheme is useful for calculating shares at receiver when the computation device is a mobile phone with low computational complexity [12].

4. CONCLUSION

Most of us already carry mobile devices in pockets and purses, which serves as evidence that they have been around for a long time, assisting individuals. A workable Android application is developed in this research scheme to implement secret sharing schemes. Mobile devices use XOR-based computation for the tasks of the dealer who creates and sends the shares and the user who decrypt the shares they receive. In order to recover n secret images

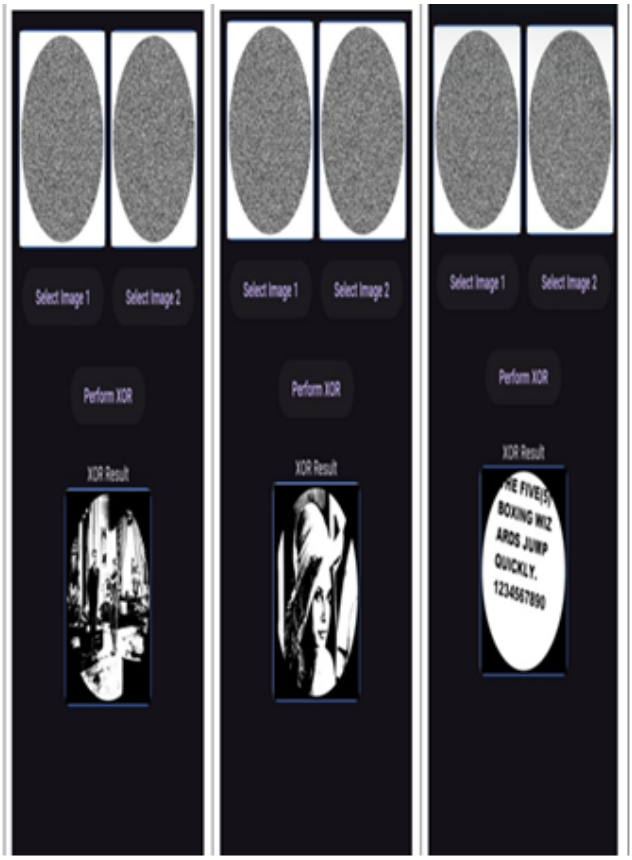

Fig. 3. The recovered multi secret images with XOR computation on universal share and rotated share images.

.

at the receiver, a universal share is computed using rotated n pie-shaped shares. The results demonstrate that the developed Android application is promising because it allows the user to decrypt secret images using a handheld device, such as a mobile phone, as opposed to using a desktop or laptop computer, which is inconvenient to carry at remote location for secret image recovery. Additionally, some applications, such as sharing a secret image of a military map with soldiers on the battlefield, use mobile phones as a computing device, retrieve the secret image, and comply with orders from higher-authorities. Additionally, by pairing with Android-powered mobile phones, the Android wear device such as Android watches can also be used to recover the secret image. In future, the proposed research technique can be enhanced by developing generalize android application which is suitable for various secret sharing schemes.

5. REFERENCES

[1] Kanchan Bisht and Maroti Deshmukh. A novel approach for multilevel multi-secret image sharing scheme. *The Journal of Supercomputing*, 77(10):12157–12191, 2021.

[2] T Jones Daniel and R Sundar Rajan. on mobile application. In *Proceedings of International Conference on Computing and Communication Systems for Industrial Applications: ComSIA 2024*, page 57. Springer Nature, 2025.

[3] Muzammil Hussain, Ahmed Al-Haiqi, Aws Alaa Zaidan, Bilal Bahaa Zaidan, M Kiah, Salman Iqbal, Shaukat Iqbal, and Mohamed Abdulnabi. A security framework for mhealth apps on android platform. *Computers & Security*, 75:191–217, 2018.

[4] Oded Kafri and Eliezer Keren. Encryption of pictures and shapes by random grids. *Optics letters*, 12(6):377–379, 1987.

[5] Yu-Ru Lin and Justie Su-Tzu Juan. Rg-based region incrementing visual cryptography with abilities of or and xor decryption. *Symmetry*, 16(2):153, 2024.

[6] Yogesh K Meghrajani, Laxmi S Desai, and Himanshu S Mazumdar. Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share. *Journal of Information Security and Applications*, 47:267–274, 2019.

[7] M. Naor and A. Shamir. Visual cryptography. In *Proc. of the Advances in Cryptology, Eurocrypt '94, Lecture Notes in Computer Science*, volume 950, pages 1–12, 1995.

[8] Hossein Nejati, Victor Pomponiu, Thanh-Toan Do, Yiren Zhou, Sahar Iravani, and Ngai-Man Cheung. Smartphone and mobile image processing for assisted living: Health-monitoring apps powered by advanced mobile imaging algorithms. *IEEE Signal Processing Magazine*, 33(4):30–48, 2016.

[9] Dipak K Rabari, Yogesh K Meghrajani, and Laxmi S Desai. *Harnessing Quantum Cryptography for Next-Generation Security Solutions*, chapter A Study of Secret Image Sharing Schemes Using Visual and Quantum Cryptography, pages 439–466. IGI Global Scientific Publishing, Hershey PA, 17033, USA, November 2024.

[10] Arjun Singh Rawat, Maroti Deshmukh, and Maheep Singh. A novel multi secret image sharing scheme for different dimension secrets. *Multimedia Tools and Applications*, 82(23):35183–35219, 2023.

[11] Neil Smyth. *Android Studio Iguana Essentials-Java Edition: Developing Android Apps Using Android Studio 2023.2. 1 and Java*. Payload Publishing, 2024.

[12] Srividhya Sridhar and Gnanou Florence Sudha. Circular meaningful shares based (k, n) two in one image secret sharing scheme for multiple secret images. *Multimedia Tools and Applications*, 77(21):28601–28632, 2018.

[13] Xiaotian Wu and Peng Yao. Boolean-based two-in-one secret image sharing by adaptive pixel grouping. *ACM Transactions on Multimedia Computing, Communications and Applications*, 19(1):1–23, 2023.