ISSN: 2182-2069 / E-ISSN: 2182-2077

Multi-Language Confidential Information Hidden in Multi-Channel Images with Unicode – ASCII Codes and Binary Signal Combination

Kudakwashe Vhito[1], and Varin Chouvatut[2*]

[1]Research Scholar, Department of Computer Science, Faculty of Science, Chiang Mai University, Thailand. kuda.vhito@gmail.com, https://orcid.org/0009-0000-4335-6929

[2*]Associate Professor, Department of Computer Science, Faculty of Science, Chiang Mai University, Thailand. varin.ch@cmu.ac.th, https://orcid.org/0009-0008-9125-4650

Received: July 07, 2025; Revised: August 19, 2025; Accepted: September 24, 2025; Published: November 28, 2025

Abstract

Encryption transforms plain text into unreadable ciphertext, while steganography hides one piece of information within another, concealing its existence. This paper introduces a novel algorithm securing information communication through a combination of image steganography and a key in binary code converted into a digital signal. The binary key that is used to generate the key is directly linked to the mapping table and it defines how the information is encrypted within the image. When concealing the secret message, the information is hidden within different color spaces (RGB, RGBA, and CMYK), and with the channels having distinct channel ranges it adds to the complexity and robustness of our encryption process. Our method supports any local language which makes it highly adaptable as it utilizes a combination of Unicode – ASCII, symbols and mathematical formulas that can be rendered using LaTeX (Tex) files. This makes it compatible with a broad range of characters and thus widely usable. The key innovation in our technique is the use of blank images as carriers of information, making it discreet thus minimizing the risk of corruption as images are prone to corruption if some information is embedded into them. A significant advancement in the field of information security has been made from this research and allowing information concealment in any color space of the sender's choice while the receiver retravels this information by both sound and mapping table just proves the flexibility of the process. Real world scenarios, academic research and secure government communication are some examples of a wide range of applications of the research.

Keywords: Encryption, Latex (Tex File), Image Steganography, Signal Processing, Information Security, Unicode – ASCII.

1 Introduction

In this information age, the art of encryption is important to safeguard sensitive information from potential threats such as eavesdroppers, cyber attackers, and unauthorized users. The concept of computer security covers several areas with confidentiality of the information being one of the most important areas. The rise of the internet has had a spotlight on the critical role encryption plays in securing data during online transmissions (Nayak & Mathur, 2021). Fundamentally encryption involves the transformation of plain, readable messages into encrypted ciphertext, rendering them unreadable without undergoing the necessary decryption process. The decryption process effectively reverses the

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 28-46.
DOI: *10.58346/JISIS.2025.I4.003*

*Corresponding author: Associate Professor, Department of Computer Science, Faculty of Science, Chiang Mai University, Thailand.

process done during encryption, returning the ciphertext to its original readable plain text (Balajee, 2011). Concerning secure information communication, two techniques come to the forefront: steganography and cryptography (Barhoumi et al., 2024; Li et al., 2020). Both have different purposes, on one hand, cryptography focuses on securing information by changing it into an unreadable format, keeping its confidentiality and integrity (Abdullah & Aziz, 2016). On the other hand, steganography goes a step further by concealing the very existence of a message within another medium, thus adding an extra layer of secrecy to communication (Hermansyah, 2023). In steganography, the most common medium is digital images as they stand out as the most popular choice for concealing information. Since digital image communication online is very common, it makes them an ideal medium for hiding sensitive data, making it challenging for even anyone to think any other form of communication is going on (Shirke & Udhayakumar, 2019). The practical use of steganography varies in different domains, let's take an example in cases such as military or intelligence operations (Zaibel et al., 2022). Steganography offers disguised communication, hiding sensitive information within another medium during the exchanges. Moreover, in countries where the internet is monitored, users can bypass the censorship by employing different ways to conceal the information making it easy to access crucial content. The method of concealment depends on the nature of information to be sent and thus defining the appropriate carrier medium becomes important (Fallahhusein et al., 2025). The simplified process of image steganography is illustrated in Figure 1.

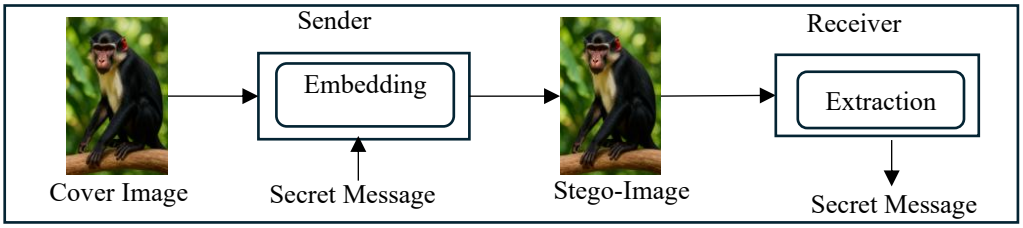


Figure 1: Comprehensive image steganographic process

There are various steganography methods such as LSB insertion, masking and cover selection. A brief discussion of some of the steganography methods is given below:

1.1 Least Significant Bit (LSB) Insertion Image

Least significant bit (LSB) insertion is the most common technique for hiding data in cover images. (Dumre & Dave, 2020) explain that the 8th bit of image bytes is replaced with a bit from a secret image or message. In color (RGB) images, 3 LSBs can be used per pixel. For example (Figure 2), hiding the number 240 in the first eight bytes of three pixels in a 24-bit image alters only 6 bits.

PIXELS:	(00100111 11101001 11001000)
	(00100111 11001000 11101001)
	(11001000 00100111 11101001)
240:	01111000
RESULT:	(00100110 11101001 11001001)
	(00100111 11001001 11101000)
	(11001000 00100110 11101000)

Figure 2: Least significant bit insertion example

Muhammad & Hikmat, 2016 proposed Hash Least Significant Bit (H-LSB). This cipher algorithm divides 8 secret message bits into 3, 3, and 2, embedding them into the cover image's RGB pixel values,

respectively, for enhanced network security. Senders use keys to encode the message before embedding, and receivers use the same keys for decryption. The general LSB algorithm for text embedding, per (Walia & Jain, 2010), involves reading the cover image and text message, converting the message to binary, calculating and replacing the LSBs of the cover image with these bits, and finally, writing the Stego image. An improved LSB algorithm for color images (Zhou et al., 2016) combines information hiding and cryptography. Experiments showed it outperforms standard LSB. (Kaul & Bajaj, 2013) embedded audio into images using LSB and wavelet transform, maximizing speech embedding. (Sinha et al.,2015) proposed combining text encryption and audio steganography for encryption. A modified Vigenère cipher that is used to encrypt text, which is then embedded into audio using LSB.

1.2 RGB Intensity-Based Image Steganography

Bagaskara et al., (2017) proposed using RGB intensity to decide the number of bits per pixel. Channels with lower values can store more bits since they affect the pixel's color less.

1.3 Spread Spectrum Image Steganography

The same authors (Bagaskara et al., 2017) also described a technique that spreads data across the frequency spectrum, reducing amplitude and making it hard to detect, thus enhancing security.

1.4 DCT-Based Image Steganography

DCT separates images into frequency components (Goel et al., 2013). Pixels are grouped into 8×8 blocks, subtracted by 128, then transformed via DCT and quantized. LSBs of DC coefficients are replaced with message bits. (Duan et al., 2020) introduced a deep learning-based method combining DCT and ECC for enhanced security. (Li Q. et al., 2020) used chaos encryption and CNN, along with GAN, to generate realistic stego images.

1.5 DWT Image Steganography

DWT splits the image into frequency components. High-frequency areas are used for embedding. (Wahab et al., 2021) used Huffman coding for text compression and DWT for cover image compression. (Abusukhon et al., 2012) proposed converting each text letter to an RGB pixel. (Singh & Jain, 2013) implemented a two-layer encryption: text-to-image and image-shuffle using a matrix scrambling technique. (AL-Laham, 2015) encrypted images via matrix transformations and double random matrix keys. (Kaur & Kumar, 2020). grouped RGB pixels separately before generating a cipher image. (Ibada et al., 2021) encrypted RGB images using a Hill algorithm with chaos-based key generation for randomness. (Kar et al., 2017) proposed using a 4D Lorenz system to split and encrypt RGB channels individually with diffusion and confusion. Similar methods are found in (Somaraj & Hussain, 2016; Yao et al., 2018; Guleria et al., 2020). Noor D. AL-Shakarchy et al. proposed a CMYK-based text-to-image algorithm using four keys per language. Unicode and crossover add encryption strength (Noor et al., 2022; Panchami et al., 2014) described compressing 16-bit Bangla and English text to 8-bit encoding using Unicode. (Abusafiya, 2021) proposed a method to compress text by mapping Unicode values and a search algorithm for compressed patterns.

The author in (Hyder et al., 2018) proposed combining transposition-based encryption algorithms with data compression by converting it into a static image and then hiding it using steganography encryption. A new algorithm was presented for grey and color medical images, which were encoded by the authors in (Kamal et al., 2021) with a new image-block splitting technique. This technique scrambled

the image blocks into a zigzag pattern then some rotation of the image, random rearrangement and lastly used diffusion using a chaotic logistic map. In another paper, a chaos-based encryption method was proposed (Arif et al., 2022) as they introduced a single substitution box for permutation-substitution, this novel idea was based on the cross-channel pixel-level scrambling enhancing the robustness. A reversible data hiding elliptic curve-based method was introduced by (Sheidani et al., 2021; Kumar et al., 2016) this method ensures that the sender and the receiver can detect the secret message. Existing adversarial encryption methods were outperformed by the research of authors (Liu et al., 2022) as they proposed an improved version of spatial and JPEG steganography. In the research of (Al-Husainy, 2017) came up with multi-level substitution and transposition idea, this was used for text to image and had a compound key to strengthen the technique.

A self-adaptive image encryption technique was proposed by the authors in (Qin et al., 2023), they based their scheme on chaos and the gravitational model. This model achieved high security but they did mention that the runtime was a limitation to address in the future. Using a high single resolution RGB image the authors (Chuang et al., 2021) proposed a data hiding encryption for 24-bit color images thus achieving an acceptable PSNR using the spatial adjacent mean proving a high embedding capacity. Another novel method was proposed by (Liao et al., 2019) as it was based on channel-dependent payload partition across RGB image, this method involved increasing pixel modification possibilities across the channels. (Guan et al., 2022) suggested an improved framework called DeepMIH of which uses a neural network for hiding multiple secret images in one cover image. It employs a fully reversible process, guided by an important map module and low-frequency wavelet loss to enhance Stego image invisibility. A novel algorithm by (Ansari et al., 2020) uses image components to store confidential data. Adaptive partitioning and data spreading across components increase security and reduce detectability.

This paper is an extension to the conference paper (Vhito & Chouvatut, 2023) the research focuses on YCbCr and HSV color spaces. The proposed method was mainly focused on encoding the ASCIII secret message within an image. The limitation of the proposed method is not having a strong key present in the encryption algorithm thus we intend to further this area and diversify our work by using different languages and color spaces. The major and fundamental contributions of the research conducted in this work are as given below:

- We combine images and signal sounds to enhance the security of concealing confidential information.
- Rather than limiting the transmission to ordinary plaintext, our method seamlessly transfers complex text and symbols, including intricate mathematical formulas.
- The international adoption of Unicode standardization at the receiver's end ensures effortless conversion of decrypted information into their respective local languages.
- Our process entails the conversion of binary string representation into discrete or continuous sound waves, broadening the spectrum of data transmission.
- During the encryption phase, we convert Unicode to ASCII to align with the image's equivalent range, facilitating the discreet embedding of characters within image pixels.
- To bolster security, we replace the conventional plaintext key with a key in the format of a sound wave, introducing a higher level of complexity and fortification.
- By utilizing multiple color space images to represent confidential information, we introduce the capability to introduce counterfeit data, enhancing the camouflage of the transmitted contents.

2 Methods

In the RGBA color space, colors are composed of red, green, blue, and alpha components. The red, green, and blue components (R, G, B) define the color itself and have a range of 0 to 255, covering the full spectrum of colors while the alpha component(A) represents the opacity of the color which ranges from 0(completely transparent) to 255(completely opaque). Thus, taking the context of RGBA the component ranges are represented as R (0-255), G (0-255), B (0-255), and A (0-255). On the other hand, looking at the CMYK color space, the individual colors are represented as cyan (C), magenta (M), yellow (Y), and key (K). The components responsible for defining the color are (C, M and Y) components. They have a range of 0 to 100 and they offer a percentage-based representation. The last component (K) also known as black represents the amount of black ink used to create the color and has a range of 0 to 100. Since CMYK uses percentage-based values (0% to 100%) this makes it suitable for color printing applications. On the other hand, the RGB color space components range from 0-255. Figure 3 shown below provides a comprehensive visual representation of our proposed model offering both the encryption from the sender side and the extraction process from the receiver's side. Additionally, the key creation process is also seen in the illustration as it is a vital part of our technique. Figure 3 serves as a valuable reference in understanding the key stage which will be further explained in this section as the key creation needs detailed explanation as it's a very important component in our proposed model.

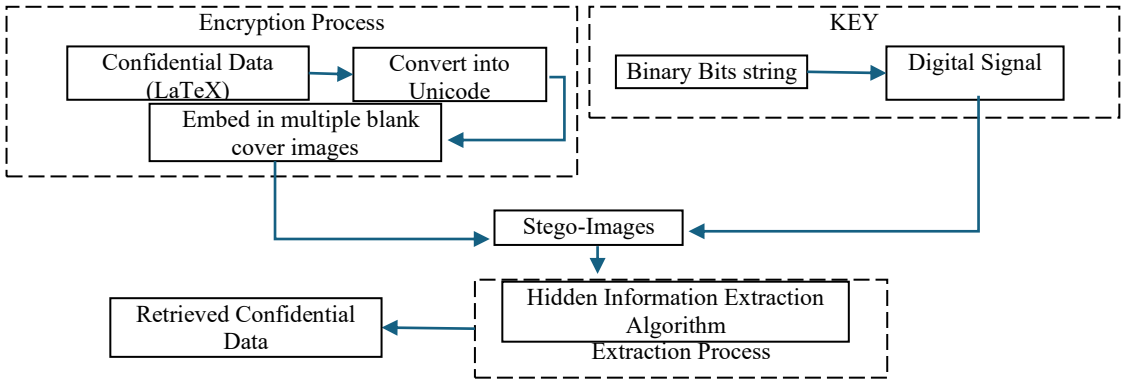


Figure 3: Comprehensive illustration of our proposed model

As seen in figure 3, the steps shown are used to conceal information from the sender and retrieved by the intended receiver. The information is spread across the different cover images across different color space formats such as RGB, RGBA, and CMYK. For better implementation, we have used a LaTeX file (Bos & McCurley, 2023). as it's easier to accommodate international languages with ease.

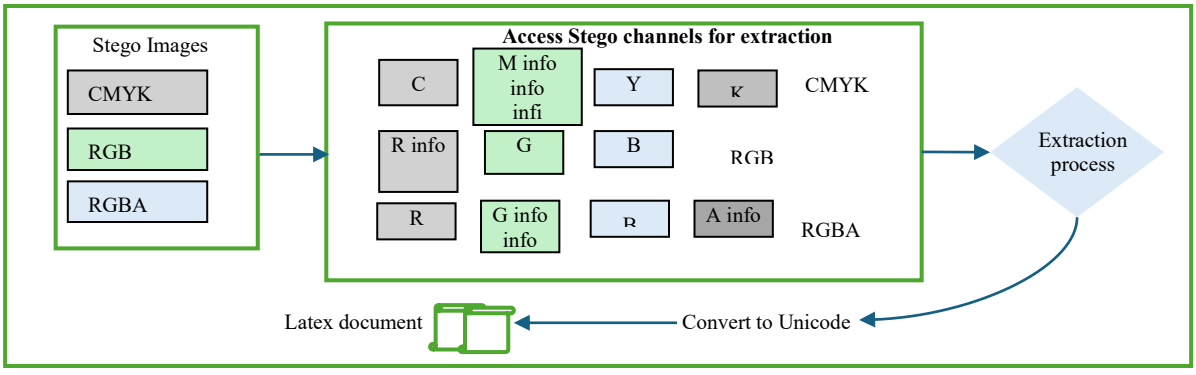


Figure 4: Flowchart of the encoding process

LaTeX provides a flexible and user-friendly platform for presenting complex data while guaranteeing compatibility with a wide range of languages. The flowchart illustrating the encoding and extraction processes for our confidential information is presented in Figure 4 and Figure 6, respectively. This choice of LaTeX format for our plaintext facilitates the seamless integration of specialized symbols, mathematical equations, and multilingual content, making it an ideal choice for our research objectives.

The process of embedding secret communication into the cover image is as follows -

Step 1: Multiple blank images are created, and the image should have different file formats and sizes.

Step 2: For each image, take the blank image and split it into its individual color channels. Once opened, a blank array of the same size as the initial blank image is created, and that represents the image channel of the Stego image. This step was repeated for all the channels.

Step 3: Convert the confidential information from the LaTeX document to Unicode (Rose et al., 2023) since we have non-English characters. Proceed to remove the "\u" characters from the converted document for added security.

Step 4: Convert the Unicode into ASCII making sure it's in the range of 0-255 for each of the characters and modify an array with the primary text values.

Step 5: Working with CMYK, it is important to remember the range of the channels, as it only allows a range of 0 to 100, meaning after four-channel randomization, iterate through the array of values, and check if it is greater than 100. If so, subtract from the initial value and store the resulting value in a separate list, signifying restoration. Figure 5 shows the subtracted and restoration array of the word "Code" given by [66,111,100,101].

Reduced array	[67,100,100,100]
Restored array	[11,0,1]

Figure 5: Example of subtracted and restoration array

When the value is exactly 100, 0 is stored in the restoration list. For all values above 100, 100 was added to a new array, representing the reduced values. The rest of the original array was then kept in the restoration list. This restoration array will be embedded in one of the channels of any given color space.

Step 6: Partition the ASCII values based on the number of channels within the corresponding image color space. To distribute the information load, we define L1 = W1·C for the first channel, and L2 = W2·C for the second channel, with W1 and W2 set to a value between 0-1 percent. For calculating the information allocation for the third channel (L3), utilize Equation (1):

$$L_3 = C - \sum_{i=1}^{3} L_i \tag{1}$$

Here, C denotes the initial secret message (information load). By calculating L3 using Equation (1) instead of relying on (2) for its computation, we ensure the precise determination of the remaining values destined for the third channel. Neglecting this accurate transmission of the third channel, often attributed to potential rounding errors stemming from fluctuating calculations in programming, which may lead to erroneous decryption, rendering the information irretrievable at the recipient's end.

$$L_3 = w_3 \cdot C = \left\{1.0 - \left(\sum_{i=1}^{2} w_i\right)\right\} \cdot C \tag{2}$$

To clarify, these round off errors arise from programming calculations and are not associated with the precise mathematical calculation of W3 as expressed in (5). Taking an example as w1 is set to 0.2 implies that L1 retains 20% of the encrypted information, while w2 is set at 0.4 meaning L2 holds 40% of the encrypted data. Therefore, the ideal mathematical computation, as determined by (5), establishes w3 as 0.4, signifying that L3 is responsible for safeguarding the outstanding 40% of the encoded information.

$$1.0 = \sum_{i=1}^{3} w_i \tag{3}$$

It's crucial to emphasize that the values of w1, w2, and w3 are customizable and employed as private or secret keys, accessible solely by the sender and recipient. From equation (3), the values should always be equal to 100 percent.

$$100\ \% = \sum_{i=1}^{3} (w_i \cdot 100)\ \% = \sum_{i} W_i \tag{4}$$

$$w_3 \cdot 100\ \% = \left[100 - \left(\sum_{i=1}^{2} (w_i \cdot 100)\right)\right]\% \tag{5}$$

This condition pertains to color spaces characterized by three channels, namely h1 –h3, each possessing potential maximum intensities denoted as h1max – h3max, respectively. Importantly, it's worth noting that this technique remains applicable even in color spaces comprising more than three color channels.

$$\left(\sum_{i=1}^{3} w_i\right) \cdot C\ \leq \sum_{j=1}^{3} h_{j,max} \tag{6}$$

Step 7: Iterate through each pixel (n, m) within the channels of the blank image:

a) If there are any remaining ASCII codes within the primary text array, assign the pixel value at index (n, m) as the following ASCII code in the array.

b) In case that every ASCII codes has been utilized, designate the pixel value at index (n, m) as 0.

c) Continue with the repetition of steps a) and b) until every pixel within the channel of the Stego image has been systematically processed.

Step 8: Provide the resultant array that represents the image channel of the Stego image. Proceed to reiterate Step 5, for the remaining two channels.

Step 9: Following the encoding of the confidential message within their individual channels, combine these channels to generate the final Stego image.

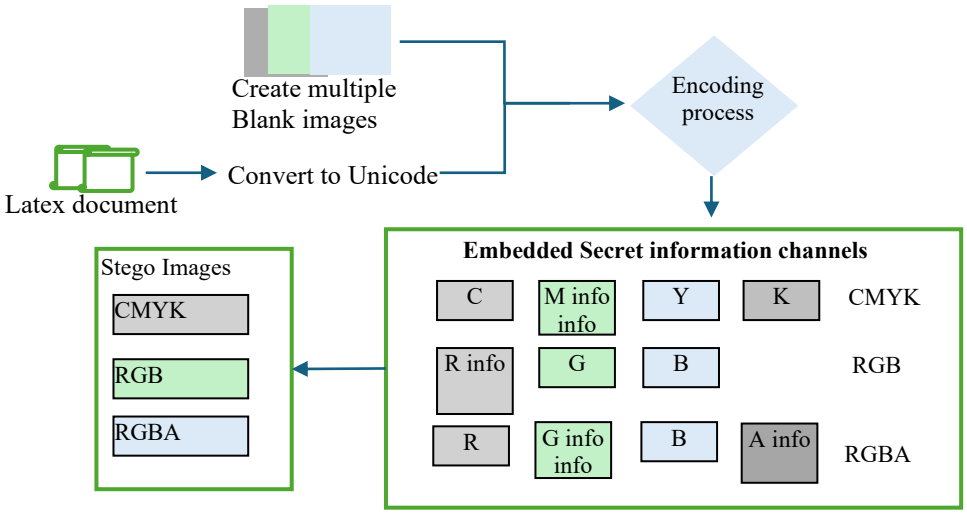


Figure 6: Flowchart of the extraction process

The process of retrieving the confidential information from the Stego image is as follows –

Step 1: Commence by taking the received Stego image. Open and divide the image into its distinct channels and preserve each channel within separate variables.

Step 2: Unify the channels of the Stego image into a singular array by aggregating the corresponding pixel values from each channel. This operation yields a new array encompassing the entire original message encoded within the Stego-image, utilize (7):

$$C = \sum_{i=1}^{3} L_i \tag{7}$$

Step 3: Initialize an empty list to collect the original values. Subsequently, iterate through the combined array, extracting non-zero values indicative of the original data embedded within the image. This step serves to recover the concealed original values.

Step 4: As a concluding action, transform the list of ASCII values into a continuous string and write this string into a text file(.txt). This file serves as a human-readable representation of the retrieved secret message, bearing a .txt file extension for convenient access and comprehension.

2.2 Digital Signal (KEY)

The advancement of our steganography methodology advances with a fundamental focus on the encryption key, which adopts the form of a binary digital signal. This signal, essentially a binary string is carefully created with the guidance of a sender-provided mapping table, this plays a fundamental role in ensuring protected communication to the intended recipient. The mapping table serves as a comprehensive reference with crucial details such as the number of images being sent, the specification of the color spaces involved and the way the counterfeit data and actual covert messages are embedded within various channels. Table 1 serves as the reference mapping table utilized for creating the digital signal along with an overview of key generation with their different stages seen in Figure 7.

This table provides an overview of the distribution of information across all images and their respective channels, while also providing insights into the allocation of concealed data. The number of images is represented by 5 bits, indicating a total of 32 images available to be sent if needed.

Table 1: Reference mapping table for digital signal.

Information Category		Number of Bits
Number of images	-	5
Color spaces of each image	Subtype RGBA	3
	Subtype CMYK	3
	Subtype RGB	3
Confidential info/fake channels of each image	Channels of RGBA	4
	Channels of CMYK	4
	Channels of RGB	4
Information partition of each image	Percentage of K1	7
	Percentage of K2	7
	Percentage of K3	7

The 3-bit representation indicates the color space type used by each image being transmitted. In the case that you have multiple images being sent, multiply by three to have the bits required to represent each image. The next 4 bits represent confidential and fake information within the channels of the color space. Essentially, this table helps distinguish which channels contain real information versus fake information.

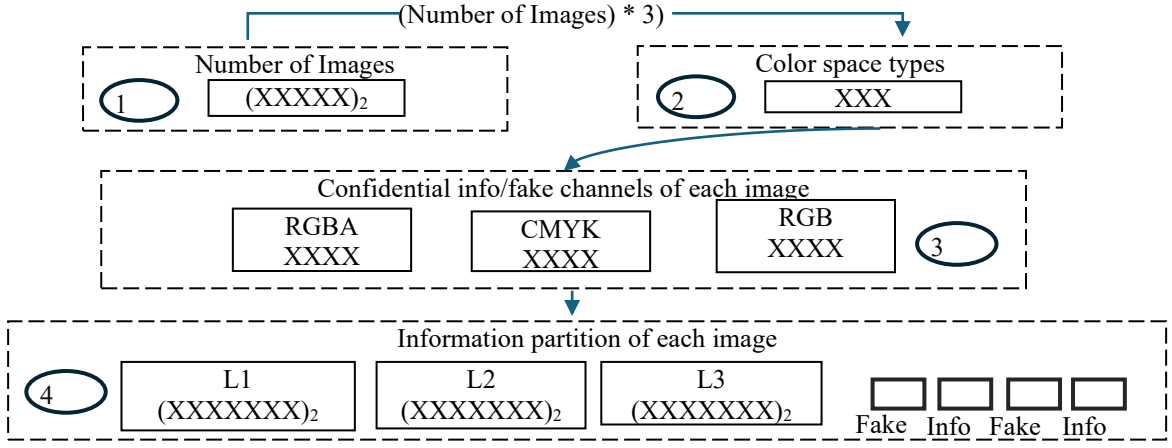


Figure 7: Overview of key generation based on mapping table

Figure 8 shows three of the color spaces utilized in our key generation algorithm, considering the RGB color space: real information resides in the green and blue channels, while the red channel holds fake data. We have introduced an additional fake channel to the RGB color space to increase complexity at this stage, making it difficult to determine the actual true capacity of channels available to hold information. By examining the CMYK color space, we observe that magenta and yellow channels are storing real information, while cyan and key(K) contain fake data. This method is extended to the RGBA color space where the red, green and alpha channels contain secret information, and the blue channel contains fake information. Lastly, the information partition of each image is represented by 7 bits, meaning that the bits can represent the values of 0-100% making it possible to represent each partition of information done in each image.

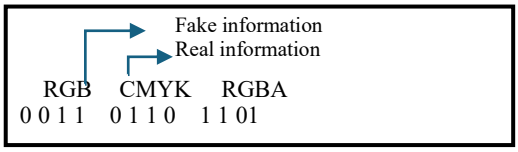


Figure 8: Flowchart for generating digital signals

This approach gives us control over where information is stored, adding complexity beyond full image encoding and making it harder for unauthorized parties to locate the exact channels used. A mapping table guides the extraction of these channels, converting the binary string into a digital signal that becomes an audible sequence sent to the recipient. Using the same table, the receiver decodes the signal, uncovering the interaction between real and false data and the complexity of the encryption. This insight is key when handling the signal's high and low frequencies. Without the mapping table, decoding the sound wave's bit-level information would be difficult.

2.3 Hierarchy Diagram of Level Security

Figure 9 diagram outlines our comprehensive security approach. It starts by manipulating plaintext data, handling Unicode, color channels, and private key offsets for confidentiality. It then manages image data, making real and fake info indistinguishable across sizes, formats, and color spaces. Key management is central, using bits for channel counts, sender's color space, secret channels, and info division ratios. Offset bits enhance security, acting like extra private keys, resulting in a robust communication framework.

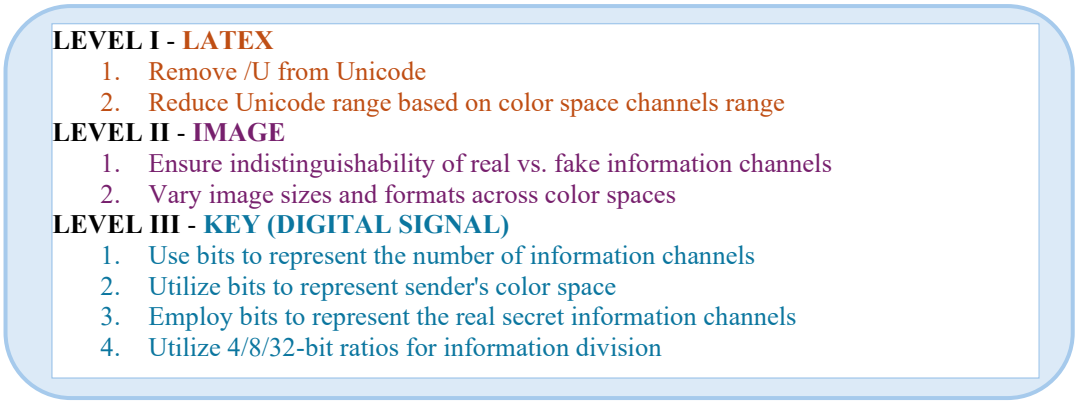


Figure 9: Hierarchy diagram of our multiple-level security

3 Results

The following section provides the experimental results and analysis in which the demonstration of the efficiency of the proposed method is given. Our proposed model for embedding and extracting the information was applied to blank images created from the different color spaces (RGB, CMYK, and RGBA). In this section, the results of our experiment are presented as stated in the methodology section. A comparative analysis based on the text files used as input and the retrieved files is provided.

3.1 Experimental Setup

For our results validation, we tested our proposed model on a system with 1.80 GHz Intel Core i3 CPU. Used Windows 11 with 8 GB Ram. Our model was implemented by Python libraries such as Pillow and OpenCV for the image processing while NumPy and Matplotlib were utilized for numerical operations and visualization respectively. Bitarray library was used for bit-level signal manipulation. For creating the (.tex) documents, we used Overleaf and Jupyter notebooks as the main development environment (Namiot, 2019). This setup thus allowed signal handling and accurate encoding and extraction operations.

3.2 Plaintext

This work is focused on confidential information within LaTeX(.tex)files. Thus demonstrating how our method is robust in handling multiple languages and complex symbols. The following figures (10-15) illustrate how the original confidential information is stored and its encoded forms within the different color spaces. On the side of retrieving and decoding the information, we consistently achieved 100% accuracy, showing that our method was reliable and prepared to handle sensitive information.

The following figure 10 demonstrates the use of both Chinese and English languages, showing the flexibility of our method. A noteworthy feature is the seamless integration of Chinese characters into the LaTeX document using Overleaf, a powerful online LaTeX editor. Figure 11 shows that, after decryption, the information correctly returns to its original formatting for both languages.

```
\Documentclass{article}
\usepackage{xeCJK}
\begin{document}
\section{前言}
这是一些文字。

\section{关于数学部分}
数学，中英文皆可以混排，You can intersperse math, Chinese and English (latin script) without adding extra environments.
這是繁體中文。
\end{document}
```

Figure 10: Concealed message in LATEX markup languages of english and chinese

1 前言
这是一些文字。

2 关于数学部分
数学，中英文皆可以混排，You can intersperse math, Chinese and English (latin script) without adding extra environments.
這是繁體中文。

Figure 11: Initial formatting of original and recovered information (chinese and english) from stego images

Pi × (%A) + Pi × 100 = PA × 100
PA = Pi × ((%A + 100) / 100)
Mean (μ): E(X) = ∫ from −∞ to ∞ of x·f(x) dx
FU(u) = P(U ≤ u) = 1 − P(U > u) = 1 − P(X1 > u, X2 > u, ..., Xn > u)
cdf of X:
F(x) = {
1 − e^(−λx) for x ≥ 0
0 for x < 0
}

Figure 12: Initial formatting of original and recovered information (mathematical formulas and complex symbols) from stego images

Figure 12 illustrates the testing of our proposed model with a diverse range of characters, some of which could have presented challenges when used in other programs. The inclusion of complex equations and symbols as seen in figure 13 code snippet, becomes not only feasible but also effortless.

Our algorithm seamlessly handles these intricate symbols without encountering any issues, demonstrating its robustness and effectiveness in working with such complex elements.

```
\documentclass[10pt] {article}
\usepackage{amsmath, amsfonts, amssymb}
\date {}
\begin{document}
\section{Formula}
$$
P_i \times (\%A) + P_i \times 100 = P_A \times 100 \\
$$
$$
P_A = P_i \left( \frac{\%A+100}{100} \right) \\
$$
\begin{tabular}{lp{8cm}}
  Mean ($\mu$): & $E(X) = \int_{-\infty}^{\infty} xf(x) dx$ \\
\end{tabular} \\
\begin{tabular}{lp{12cm}}
  $F_U(u)$ & $= P(U \leq u) = 1 - P(U>u) = 1 - P(X_1>u, X_2>u, ..., X_n>u)$ \\
\end{tabular} \\

\underline{cdf of X} \\
$F(x)=$
\begin{cases}
  1 - e^ {-\lambda x} & x \geq 0 \\
  0 & x < 0
\end{cases}
\end{document}
```

Figure 13: Hidden data of mathematical formulas and complex symbols

```
\documentclass[11pt,a4paper]{report}
\usepackage[utf8]{inputenc}
\usepackage{arabtex}
\usepackage[arabic]{babel}
\author{سالم البوزيدي}
\begin{document}

\section{تاريخ}
\begin{otherlanguage}{Arabic}
يعود تاريخ علوم الحاسوب إلى اختراع أول حاسوب رقمي حديث. فقبل العشرينات من القرن العشرين، كان مصطلح حاسوب
\textLR{Computer} يشير إلى أي أداة بشرية تقوم بعملية الحسابات. ما هي القضايا أو الأشياء التي يمكن لآلة أن
تحسبها باتباع قائمة من التعليمات مع ورقة وقلم، دون تحديد للزمن اللازم ودون أي مهارات أو بصيرة (ذكاء)؟ وكان أحد
دوافع هذه الدراسات هو تطوير آلات حاسبة \textLR{computing machines} يمكنها إتمام الأعمال الروتينية
والعرضة للخطأ البشري عند إجراء حسابات بشرية.
\end{otherlanguage}
\end{document}
```

Figure 14: Hidden communication within LaTeX markup arabic language

تاريخ

يعود تاريخ علوم الحاسوب إلى اختراع أول حاسوب رقمي حديث. فقبل العشرينات من القرن العشرين، كان مصطلح حاسوب يشير إلى أي أداة بشرية تقوم بعملية الحسابات. ما هي القضايا أو الأشياء التي يمكن لآلة أن تحسبها باتباع قائمة من التعليمات مع ورقة وقلم، دون تحديد للزمن اللازم ودون أي مهارات أو بصيرة (ذكاء)؟ وكان أحد دوافع Computer هذه الدراسات هو تطوير آلات حاسبة computing machines يمكنها إتمام الأعمال الروتينية والعرضة للخطأ البشري عند إجراء حسابات بشرية.

Figure 15: Initial formatting of original and recovered information (arabic) from stego images

Figure 14 shows the code snippet layout of our secret information in the .tex file. Figure 15 demonstrates the algorithm's proficiency with Arabic text, highlighting its flexibility and ability to handle linguistic complexity. The results indicate a 100% accuracy rate in retrieving encoded data at both character and word levels, confirming the method's precision and reliability.

3.3 Digital Signal

Based on the general outline of the mapping table, we can generate a key for the documents illustrated in Figures 11, 12, and 15 (LaTeX, n.d.). The digital signal key generation process is illustrated in Figure 16. The first image includes information containing English and Chinese characters, stored in the RGBA color space. In the RGBA color space, secret information is stored within the green and alpha channels, while fake information is found in the red and blue channels. The text is partitioned into L1 and L2 sections, representing 30% and 70% respectively. The second image contains mathematical and complex symbols, embedded in the CMYK color space. Real information is stored in the Cyan (C), Yellow (Y), and Key (K) channels, whereas Magenta contains fake information. The text partition is distributed evenly, with 20% allocated to both L1 and L3 and 60% to L2. Lastly, the third image features Arabic Language text, embedded in the RGB color space. Information is present in the green and blue channels, while the remaining channels carry fake data. In terms of the partition, L1 carries 40% of the image while the L2 partition represents 60% of the information. The digital sound can now be created from all the bits together.

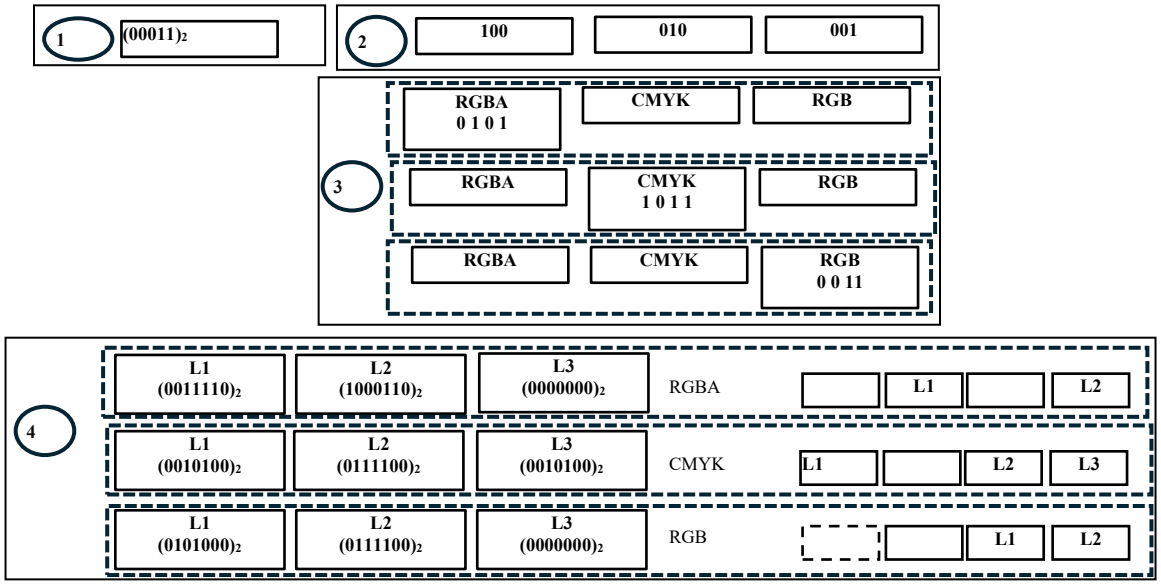
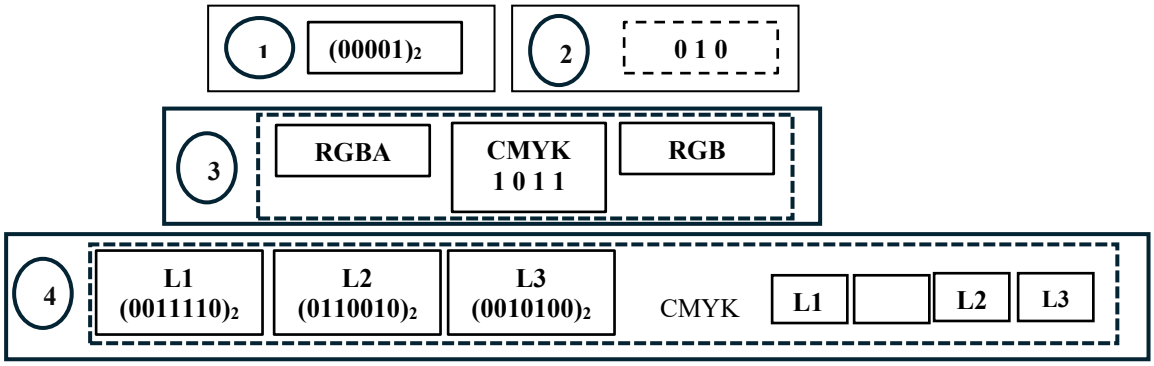
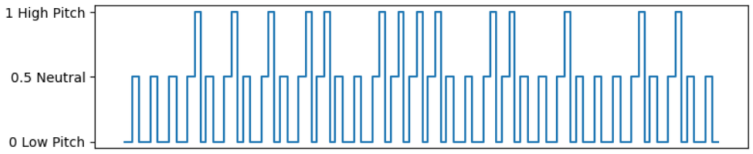


Figure 16: Digital signal graph of the Key

Given that we only want to send the mathematical and complex symbols in Figure 16 as the sole text in a communication channel, using our technique we can create the key for the single image, as depicted in (Figure 17a). The generated digital signal is illustrated in (Figure 17b), this signal is transmitted to the receiver as variations in amplitude between high, neutral and low-pitched noises. The receiver must decode these variations using the shared mapping table to get any meaning from the sound to decode the original information from the image. The final binary code: 00001 010 1011 0011110 0110010 0010100



(a) Single image key



(b)

Figure 17: Digital signal graph of the Key

The sound received by the recipient, representing our image-based information concealment method, may seem like random high and low-pitched tones to outsiders. Without the mapping table, it holds no meaning, ensuring secure transmission. Table 2 summarizes experimental results, showing encrypted and extracted data across different image color spaces. Information was evenly split and embedded using Unicode into specific color channels—Green and Red in RGB, Y and K in CMYK, and Alpha and Blue in RGBA. We carefully adjusted values to stay within acceptable color space ranges. The transmitted content, shown in Figures 10, 13, and 14, includes LaTeX documents in Chinese and Arabic, confirming our method's effectiveness across languages and character sets, and proving its robustness and universality.

Table 2: Two image encryption and extraction characteristics comparison

Color Space Stego-image	Image size	Secret Message File format	No. of Characters of Confidential Message	No. of Characters Retrieved	Extraction Accuracy (%)
RGB	128×128	.tex	3881	3881	100.0
CMYK	512×512	.tex	2781	2781	100.0
RGBA	128×128	.tex	1045	1045	100.0
RGB	512×512	.tex	2345	2345	100.0
CMYK	128×128	.tex	2928	2928	100.0
RGBA	512×512	.tex	4212	4212	100.0

Table 3 summarizes our experimental results using three images for encryption and extraction. It compares hidden message properties across different file formats, image dimensions, message sizes, and encoding methods, while also evaluating retrieval accuracy. The results are highly promising, showing a consistent 100% accuracy rate, highlighting the strength and reliability of our approach for secure data hiding and recovery across varied scenarios.

Table 3: Three image encryption and extraction characteristics comparison

Color Space Stego-Image	Image size	Secret Message File format	No. of Characters of Confidential Message	No. of Characters Retrieved	Extraction Accuracy (%)
RGB	128×128	.tex	3881	3881	100.0
CMYK	512×512	.tex	2781	2781	100.0
RGBA	128×128	.tex	1045	1045	100.0
RGB	512×512	.tex	2345	2345	100.0
CMYK	128×128	.tex	2928	2928	100.0
RGB	512×512	.tex	4212	4212	100.0

4 Discussions

Our research presents an innovative technique for embedding and extracting information across RGB, CMYK, and RGBA color spaces, offering flexibility beyond conventional steganography, which typically relies on a single color space. By allowing selection of specific channels for encryption, our method enhances control and adaptability. Unlike traditional approaches focused on distortion metrics like SNR and MSE, we prioritize the accurate retrieval of the original data. However, our technique can still be integrated with traditional methods using a cover image, making it compatible with standard evaluation practices. A defining strength of our method is the use of blank images for data hiding. This not only simplifies control over image properties (e.g., size, format) but also reduces suspicion, boosting both security and flexibility. The encoding keys, L1 and L2, can be freely chosen as long as they sum to 1. Our experiments confirm a consistent 100% accuracy in data extraction across all color models. Our model supports multiple languages with a mix of complex symbols enabled by Unicode. Overleaf makes it easy to write our content in LaTeX format, thus it's very adaptable. The other side of our model is based on an audio-based steganography, and having the mapping table enables proper decoding of information from the receiver side.

5 Conclusion

We propose a novel steganography technique that secures our information exceptionally well, while being very versatile in implementation across the various color spaces. One of the key features of our model is the ability to choose any color space the sender wants within an image to send the information. That combination, with the addition of blank images, made our model achieve 100% accuracy, as the information was extracted from the receiver's side. The wide applicability of our technique in dealing with different sensitive materials and multiple languages also further indicates how practical it can be used by any person for communication purposes. On the other hand, while our study provides valuable insights, we believe further research is needed to explore additional applications and refine the technique even further. Overall, this work does contribute to the advancements of secure communication, and the techniques have a strong potential when applied in academic and real-world situations.

Declaration of Competing Interest

The authors declare that they have no competing financial interests or conflicts of interest to report regarding the presented study.

References

[1] Abdullah, A. M., & Aziz, R. H. H. (2016). New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm. *International Journal of Computer Applications*, *143*(4), 11-17. https://doi.org/10.5120/ijca2016910143

[2] AbuSafiya, M. (2021, July). A Text Search Algorithm in Compressed Text. In *2021 International Conference on Information Technology (ICIT)* (pp. 589-591). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491642

[3] Abusukhon, A., Talib, M., & Ottoum, I. (2012). Secure network communication based on text-to-image encryption. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *1*(4), 263-271.

[4] Al-Husainy, M. A. F. (2016). New Implementation of Text-To-Image Encryption Using Multilevel Substitution and Transposition Operations. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(9).

[5] AL-Laham, M. M. (2015). Encryption-decryption RGB color image using matrix multiplication. *International Journal of Computer Science & Information Technology*, *7*(5), 109-119. https://doi.org/10.5121/ijcsit.2015.7508

[6] Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2020). A multiple-format steganography algorithm for color images. *IEEE Access*, *8*, 83926-83939. https://doi.org/10.1109/ACCESS.2020.2991130

[7] Bagaskara, J. A., Purboyo, T. W., & Nugrahaeni, R. A. (2017). Analysis of JPEG Image Steganography Using SPread Spectrum Method. *International Journal of Applied Engineering Research*, *12*(23), 13944-13950.

[8] Balajee, M. (2011). UNICODE and colors integration tool for encryption and decryption. *International Journal on Computer Science and Engineering (IJCSE)*, 3(3), 1197–1202.

[9] Barhoumi, E. M., Charabi, Y., & Farhani, S. (2024). *Detailed guide to machine learning techniques in signal processing. Progress in Electronics and Communication Engineering, 2 (1), 39–47*.

[10] Bos, J. W., & McCurley, K. S. (2023). LaTeX, metadata, and publishing workflows. https://doi.org/10.48550/arXiv.2301.08277

[11] Chuang, Y. H., Lin, B. S., Chen, Y. X., & Shiu, H. J. (2021). Steganography in RGB images using adjacent mean. *IEEE access*, *9*, 164256-164274. https://doi.org/10.1109/ACCESS.2021.3132424

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A new high-capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access*, *8*, 25777-25788. https://doi.org/10.1109/ACCESS.2020.2971528

[12] Dumre, R., & Dave, A. (2021, July). Exploring LSB steganography possibilities in RGB images. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICCCNT51525.2021.9579588

[13] Fallahhusein, M., Fernandes, R. B., Naga Raju, M., ugli, I. S. S., Nijaguna, G. S., & Udayakumar, R. (2025). Open Access Service Models: Impact on Information System Design. *Indian Journal of Information Sources and Services, 15*(2), 148–153. https://doi.org/10.51983/ijiss-2025.IJISS.15.2.20

[14] Goel, S., Rana, A., & Kaur, M. (2013). A review of comparison techniques of image steganography. *IOSR Journal of Electrical and Electronics Engineering, 6*(1), 41–48. https://doi.org/10.9790/1676-0614148

[15] Guan, Z., Jing, J., Deng, X., Xu, M., Jiang, L., Zhang, Z., & Li, Y. (2022). DeepMIH: Deep invertible network for multiple images hiding. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(1), 372-390. https://doi.org/10.1109/TPAMI.2022.3141725

[16] Guleria, V., Sabir, S., & Mishra, D. C. (2020). Security of multiple RGB images by RSA cryptosystem combined with FrDCT and Arnold transform. *Journal of Information Security and Applications*, *54*, 102524. https://doi.org/10.1016/j.jisa.2020.102524

[17] Hermansyah, Y. (2023). Assessing the impact of communicative artificial intelligence-based accounting information systems on small and medium enterprises. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(3), 230-239. https://doi.org/10.58346/JOWUA.2023.I3.017

[18] Hyder, A., Dhande, M., Dharod, K., Lohar, M., & Makan, K. (2018, April). Text to Image Encryption Using 16* 16 Playfair Cipher and Dynamic Color Channel Selection Technique. In *2018 3rd International Conference for Convergence in Technology (I2CT)* (pp. 1-4). IEEE. https://doi.org/10.1109/I2CT.2018.8529718

[19] Ibada, A. J., Ehkan, P., Ngadiran, R., Hammood, D. A., & Alkhayyat, A. (2021, July). Rgb image encryption using hill algorithm and chaos system. In *Journal of Physics: Conference Series* (Vol. 1962, No. 1, p. 012061). IOP Publishing. https://doi.org/10.1088/1742-6596/1962/1/012061

[20] Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *Ieee Access*, *9*, 37855-37865. https://doi.org/10.1109/ACCESS.2021.3063237

[21] Kar, M., Mandal, M. K., & Nandi, D. (2017, November). RGB image encryption using hyper chaotic system. In *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 354-359). IEEE. https://doi.org/10.1109/ICRCICN.2017.8234534

[22] Kaul, N., & Bajaj, N. (2013). Audio in image steganography based on wavelet transform. *International Journal of Computer Applications*, *79*(3), 7-10. https://doi.org/10.5120/13719-1502

[23] Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*(1). https://doi.org/10.1007/s11831-018-9298-8

[24] Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal processing, 125,* 187-202. https://doi.org/10.1016/j.sigpro.2016.01.017

[25] Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., Xian, Y., & Shi, Y. (2020). A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks. *IEEE Access*, *8*, 168166-168176. https://doi.org/10.1109/ACCESS.2020.3021103

[26] Liao, X., Yu, Y., Li, B., Li, Z., & Qin, Z. (2019). A new payload partition strategy in color image steganography. *IEEE transactions on circuits and systems for video technology*, *30*(3), 685-696. https://doi.org/10.1109/TCSVT.2019.2896270

[27] Liu, M., Song, T., Luo, W., Zheng, P., & Huang, J. (2022). Adversarial steganography embedding via stego generation and selection. *IEEE Transactions on Dependable and Secure Computing*, *20*(3), 2375-2389. https://doi.org/10.1109/TDSC.2022.3182041

[28] Namiot, E. (2019). Using LaTeX for chemical formulas. *International Journal of Open Information Technologies, 7*(8), 105-108.

[29] Nayak, P., & Mathur, D. (2021). Evaluating the Impact of Social Media Algorithms on Information Dissemination. *International Academic Journal of Innovative Research, 8*(2), 21–24.

[30] Noor, N. S., Hammood, D. A., Al-Naji, A., & Chahl, J. (2022). A fast text-to-image encryption-decryption algorithm for secure network communication. *Computers*, *11*(3), 39. https://doi.org/10.3390/computers11030039

[31] Qin, Q., Liang, Z., Liu, S., & Zhou, C. (2023). A self-adaptive image encryption scheme based on chaos and gravitation model. *IEEE Access*, *11*, 47873-47883. https://doi.org/10.1109/ACCESS.2023.3267485

[32] Rose, S. J., Ozkaya, U., Yasmin, S., Jabin, S., Hasan, R., & Kabir, E. (2023). An Efficient Unicode encoded in UTF-16 text cryptography based on the AES algorithm. *Cryptology ePrint Archive*.

[33] Sheidani, S., Mahmoudi-Aznaveh, A., & Eslami, Z. (2021). CPA-secure privacy-preserving reversible data hiding for JPEG images. *IEEE Transactions on Information Forensics and Security*, *16*, 3647-3661. https://doi.org/10.1109/TIFS.2021.3080497

[34] Shirke, S., & Udayakumar, R. (2019, April). Lane datasets for lane detection. In *2019 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0792-0796). IEEE. https://doi.org/10.1109/ICCSP.2019.8698065

[35] Singh, S., & Jain, A. (2013). An enhanced text to image encryption technique using RGB substitution and AES. *International Journal of Engineering Trends and Technology (IJETT)*, *4*(5), 2108-2112.

[36] Sinha, N., Bhowmick, A., & Kishore, B. (2015). Encrypted information hiding using audio steganography and audio cryptography. *International Journal of Computer Applications, 112*(5), 49–53.

[37] Somaraj, S., & Hussain, M. A. (2016, February). A novel image encryption technique using RGB pixel displacement for color images. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)* (pp. 275-279). IEEE. https://doi.org/10.1109/IACC.2016.59

[38] Vhito, K., & Chouvatut, V. (2023, June). Steganography with adaptable separate encrypted code of hidden confidential information. In *2023 20th International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 523-528). IEEE. https://doi.org/10.1109/JCSSE58229.2023.10202145

[39] Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE access*, *9*, 31805-31815. https://doi.org/10.1109/ACCESS.2021.3060317

[40] Yao, H., Liu, X., Tang, Z., Hu, Y. C., & Qin, C. (2018). An improved image camouflage technique using color difference channel transformation and optimal prediction-error expansion. *IEEE Access*, *6*, 40569-40584. https://doi.org/10.1109/ACCESS.2018.2858858

[41] Zaibel, H. H., Dahi, K. J., & Maktouf, N. A. (2022). The Impact of Knowledge Management in Developing Administrative Creativity through the Role of Mediator for Information Technology: An Exploratory Study of the Opinions of a Sample of Administrative Leaders and Teachers of the Oil Training Institute / Bas. *International Academic Journal of Social Sciences, 9*(2), 183–193. https://doi.org/10.9756/IAJSS/V9I2/IAJSS0927

[42] Zhou, X., Gong, W., Fu, W., & Jin, L. (2016, June). An improved method for LSB based color image steganography combined with cryptography. In *2016 IEEE/ACIS 15th international conference on computer and information science (ICIS)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICIS.2016.7550955

Authors Biography

Kudakwashe Vhito is pursuing a Master's degree in Computer Science at Chiang Mai University, Chiang Mai, Thailand. He holds a Bachelor's degree in Computer Science from the University of St. Thomas of Mozambique. He is a Research Associate (Software Engineer). His main areas of research interest are Image and Signal Processing, Computer Vision, Data Security, and Machine Learning.

Varin Chouvatut, Ph.D., is an Associate Professor in the Department of Computer Science of the Faculty of Science at Chiang Mai University (CMU) in Chiang Mai, Thailand. She was awarded a Bachelor's degree in Computer Engineering with Second Class Honors from the Department of Computer Engineering of the Faculty of Engineering at King Mongkut's University of Technology Thonburi (KMUTT) in Bangkok, Thailand. She also obtained a Master's degree in Computer Engineering from the Computer Engineering Department at KMUTT. Finally, she was awarded a Doctor of Philosophy in Electrical and Computer Engineering (International Program) with GPA 4.00 from the Computer Engineering Department at KMUTT. Her research interests include (but not limited to) Computer Vision, 2D/3D Motion Processing, 3D Reconstruction, Image Processing, Machine Learning, Artificial Intelligence, Medical Imaging Analysis, Augmented and Virtual Reality, Computer Graphics, and Web-based Applications. She actively contributes to multidisciplinary research and innovation across domains.