JEECS (Journal of Electrical Engineering and Computer Sciences)
Vol. 10, No. 2, December 2025, pp. 142-151
e-ISSN: 2579-5392 p-ISSN: 2528-0260

SmartNotes Encrypted with Hybrid Cryptography Combining Rivest Cipher 4 and XChaCha20

Elizabeth Piscelia Kusuma, Aqeela Nashwa Naysilla, Bagas Dwi Yulianto

Universitas Pignatelli Triputra, Jl. Duwet Raya No.I, Karangasem, Kec. Laweyan, Kota Surakarta, Indonesia

Article Info

Article history:
Received: 28 September 2025
Revised: 31 October 2025
Accepted: 3 November 2025

Keyword:
RC4
XChaCha20
ChaCha20
SmartNotes
Cryptography

Abstract

Digital note-taking applications serve as essential tools for personal information management, presenting opportunities for enhanced security mechanisms to protect sensitive data. Most current solutions depend on server-side processing, creating potential vulnerabilities and privacy concerns. However, a robust solution that fully executes hybrid encryption on the client-side to seamlessly protect both text and image data within a single application remains unexplored. This study introduces SmartNotes, a web-based application safeguarding text and image notes through an innovative hybrid encryption system synergistically combining RC4 and XChaCha20 algorithms. A key contribution is the full client-side execution of encryption–decryption processes, eliminating server dependencies and significantly reinforcing data confidentiality. The hybrid design strategically utilizes RC4 for rapid data processing and XChaCha20 for robust cryptographic protection, creating an optimal balance between performance and security. System performance was rigorously evaluated using seven private datasets under diverse key conditions. Testing methodology included comprehensive assessment of processing speed, data integrity verification, and resistance against unauthorized access attempts. Results demonstrated flawless data restoration across all test cases, validating robustness and reliability. Encryption averaged 1.5 seconds, while decryption required 20.20 seconds metrics well-suited for practical web environments. These findings affirm SmartNotes delivers a secure, autonomous, user-centric solution for digital note management, advancing applied cryptography through a novel client-side hybrid encryption paradigm. This approach successfully balances strong security with practical performance, making it suitable for securing data in everyday web applications.

Corresponding author:
Bagas Dwi Yulianto, bagas19.yulianto@gmail.com

DOI: https://doi.org/10.54732/jeecs.v10i2.5

1. Introduction

Digital notes serve as essential tools for efficiently storing personal information, including sensitive data such as passwords, financial records, and confidential documents. With the growing adoption of web-based applications accessible across multiple devices [1], the demand for advanced data security mechanisms has become increasingly critical to safeguard user privacy. Secret key-based encryption stands as a cornerstone of data protection, ensuring exclusive user access through cryptographic keys [2]. When implemented directly on the client side [3], this approach enhances security by preventing raw data transmission and optimizes efficiency in processing both text and image content.

Among cryptographic solutions, RC4 [4], delivers exceptional speed and lightweight efficiency, making it ideal for resource-constrained web environments. Complementing this, XChaCha20 [5] provides state-of-the-art security through its 256-bit key, 192-bit nonce and HChaCha20-based keystream generation, ensuring robust protection against evolving cryptographic threats [6]. The strategic integration of

XChaCha20's advanced security framework with RC4's rapid processing capabilities establishes a complementary synergy, achieving an optimal equilibrium between computational performance and data protection.

Previous research has predominantly explored various cryptographic approaches with specific limitations. The study by R.K. Abdullah et al. [7] discusses implementing AES-RSA hybrid encryption for salary slip distribution system, but this solution remains dependent on server-side processing which creates centralized risk. Research by W.B. Nugroho et al. [8] develops digital image encryption using ChaCha20 that is robust, but focuses only on image data without considering hybrid approach with other algorithms. The work of A.R. Nurjaman and S. Umaroh [9] explores the combination of RC4 and SHA3-512 for database security, but the implementation is limited to text and does not cover multimedia content. P.S. Ramadhan et al. [10] investigates transaction data security using AES and RC4, but does not integrate XChaCha20 which offers significant security enhancement. Meanwhile, I.K.W.A.P. Ambara and B.G.K. Yudistira [3] analyze the effectiveness of client-side encryption on Google Drive, but this research does not explore the hybrid RC4-XChaCha20 architecture. Furthermore, most existing solutions remain dependent on server-side processing [11], introducing operational dependencies and potential attack surfaces [12]. This gap underscores the significant opportunity to innovate a fully client-side hybrid encryption framework capable of comprehensively and autonomously securing multimodal data like text and images.

Addressing this need, the present study introduces SmartNotes, a web-based digital note-taking application implementing a novel hybrid encryption system [13] that strategically merges RC4 and XChaCha20. By executing all cryptographic processes entirely on the client side via JavaScript, SmartNotes eliminates server dependencies while ensuring end-to-end data privacy. The research utilizes seven distinct private datasets comprising various text and image formats collected directly from user inputs, including personal notes, documents, and images with sizes ranging from 100 KB to 1.5 MB, to ensure comprehensive evaluation under realistic conditions. The system employs layered encryption [14] to protect both text and image notes, which were evaluated with rigorous evaluation of accuracy, processing speed, and key-input resilience. This research pioneers a client-side hybrid encryption paradigm for digital notes, delivering a secure, efficient, and autonomous platform for personal information protection [15].

2. Research Methodology

This research addresses the growing demand for enhanced security in digital note-taking applications by developing a robust protection system to safeguard sensitive information. To achieve this, a hybrid encryption system [16] strategically combining RC4 and XChaCha20 was designed and implemented into a web-based application using HTML, CSS, and JavaScript. The overall research flow is presented in Figure 1.

2.1 Research Flowchart

Figure 1 illustrates the systematic research methodology comprising five key stages. Each stage is elaborated as follows:

- Test Data Determination: This initial stage involved preparing seven distinct datasets with various text and image formats collected from genuine user inputs to simulate real-world usage scenarios.
- Algorithm Selection: This stage focused on evaluating and selecting appropriate cryptographic algorithms, ultimately choosing RC4 for its high-speed processing capabilities and XChaCha20 for its robust security features with 256-bit key and 192-bit nonce.
- System Implementation: The development stage encompassed building the web-based application using HTML, CSS, and JavaScript, integrating the hybrid encryption framework with full client-side execution.
- Encryption-Decryption Testing: Comprehensive testing was conducted using all prepared datasets under various key conditions, including both correct and incorrect key scenarios to validate system functionality and security mechanisms.
- System Evaluation: The final stage involved rigorous assessment of system performance metrics including processing speed, data integrity verification, accuracy, and key-input resilience across all test cases.

The sequential execution of these stages ensured systematic development and thorough validation of the SmartNotes application, providing a structured approach to achieving the research objectives.

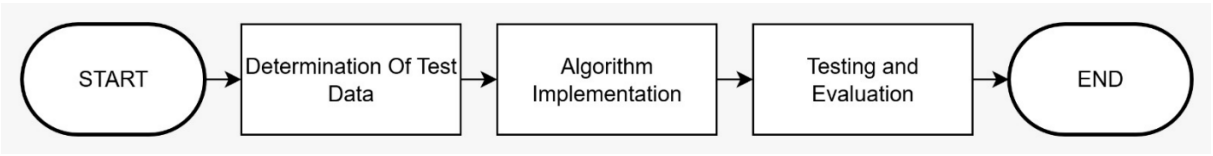


Figure 1. Research Flowchart

2.2 Test Data

Seven private datasets were used as test data, consisting of text-only notes and notes combining text with images [17]. The datasets were collected from actual user inputs with the following specifications:

- Data Sources: User-generated notes and personal images
- Data Quantity: 7 distinct datasets
- Data Types: 2 text-only datasets, 5 text+image datasets
- Text Content: 50-700 characters per dataset
- Image Files: JPG/PNG formats, 100 KB - 1.5 MB

Private data was used to maintain confidentiality and control experimental variables. Each dataset tested encryption-decryption accuracy with both correct and incorrect keys.

2.3 Algorithms

The encryption process employs a sophisticated two-layer approach [18]. Initially, RC4 generates a pseudorandom keystream using the Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA), encrypting plaintext via XOR operations. To achieve an optimal balance between speed and comprehensive security, the intermediate ciphertext undergoes secondary encryption using XChaCha20, which leverages a 192-bit nonce and HChaCha20 function to derive a cryptographically strong subkey. Decryption follows the reverse sequence, commencing with XChaCha20 and proceeding with RC4, as illustrated in Figure 2

Encryption Process (Left Side):

The encryption begins when the user inputs note content and provides a secret key. The system first checks if image data is present. For text-only notes, RC4 encryption processes the data directly using the provided key. When images are included, the system converts them to Base64 format before applying RC4 encryption. The RC4-encrypted output then undergoes secondary encryption using XChaCha20, which utilizes the HChaCha20 process for subkey generation and performs 20 rounds of ChaCha permutation. The final hybrid-encrypted data is stored locally in the system.

Decryption Process (Right Side):

Decryption initiates when the user selects an encrypted note and provides the decryption key. The system retrieves the hybrid-encrypted data from local storage and begins with XChaCha20 decryption, reversing the ChaCha20 permutation process. The intermediate result then undergoes RC4 decryption using the same key. For notes containing images, the system reconverts the Base64 data back to image format. The final output displays the original note content, successfully restoring both text and images to their pre-encrypted state.

The system incorporates a validation mechanism where failed JSON parsing due to incorrect keys triggers error messages, providing integrated security against unauthorized access [19].

2.3.1 RC4 Algorithms

The RC4 algorithm [20] is a renowned stream cipher that efficiently generates a pseudorandom keystream and encrypts data byte-by-byte using XOR operations.

The RC4 process comprises four optimized steps:

- Initialization of array S
- Key setup via the Key Scheduling Algorithm (KSA)
- Keystream generation using the Pseudo-Random Generation Algorithm (PRGA), and
- Encryption/decryption through XOR operations between plaintext and the keystream.

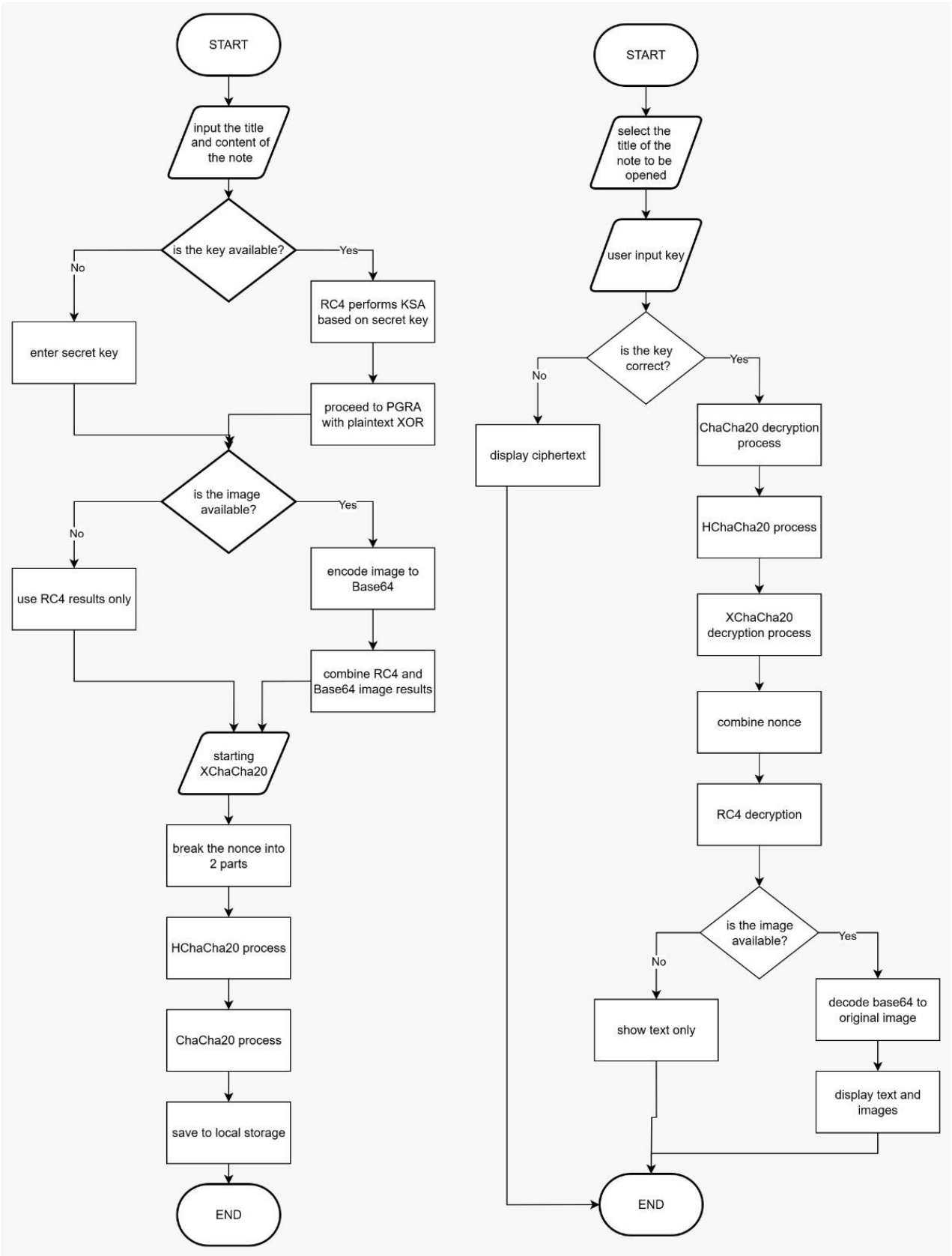


Figure 2. Implementation Flow of RC4 and XChaCha20 (left: encryption, right: decryption)

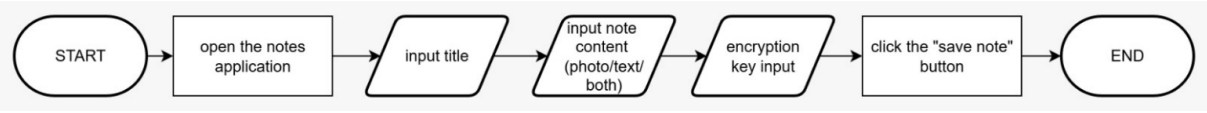


Figure 3. SmartNotes Usage Scheme

2.3.2 XChaCha20 Algorithms

XChaCha20 represents an advanced evolution of ChaCha20, utilizing a 192-bit nonce to deliver superior cryptographic security.
The algorithm executes three critical steps:

- Subkey generation through the HChaCha20 process
- State reinitialization and ChaCha permutation over 20 rounds to produce the keystream block, and
- Encryption via XOR operations between plaintext and the keystream generated by the ChaChaBlock function.

2.4 Usage Scheme

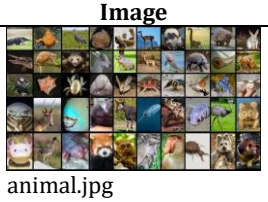
As depicted in Figure 3, application usage commences with the user entering a note title and content, supplemented by an optional image attachment. The user then inputs an encryption key serving as a fundamental data protection mechanism before clicking the Save Note button to store the encrypted note [21]. To retrieve a note, the user selects the title from the list and enters the decryption key. The system employs a dynamic security response for incorrect keys, updating the displayed ciphertext based on failed attempts to prevent unauthorized access. Upon correct key entry, the system seamlessly restores the original note content, including text and images. This mechanism ensures robust protection of personal data [22] while enabling efficient access for authorized users and facilitating comparative analysis of pre- and post-encryption/decryption states.

3. Results and Discussions

3.1 Results

This study evaluated the performance of a hybrid encryption algorithm (RC4 and XChaCha20) in processing both text and image data by measuring computation time [23] across various scenarios. The results showed that the system was able to execute both encryption and decryption processes efficiently with consistent execution times.

Table 1. *Test Data*

Plaintext		Description	
Text	**Image**	**Text Length**	Image Size
Animals are diverse living beings. They play key roles in nature, from tiny insects to large mammals, each with unique traits and behaviors.	 animal.jpg	151 character	106 kb
Tire repair is a service that fixes punctured or damaged tires. Using tools like patches or plugs, workers seal leaks to restore tire function. It's essential for vehicle safety, preventing accidents caused by flat or leaking tires, and ensuring smooth driving on the road.	 tire.jpg	303 character	192 kb
Mountain scenery offers breathtaking views with towering peaks, lush green valleys, and crisp, fresh air. The landscape is often covered with forests, rivers, and sometimes snow-capped summits that glisten under the sunlight. It brings a sense of peace and wonder, making it a favorite destination for nature lovers, hikers, and	 view.jpg	512 character	1.13 mb

photographers seeking tranquility and inspiration in the beauty of the natural world.			
Fish are aquatic animals that live in both freshwater and saltwater environments. They come in a wide variety of shapes, sizes, and colors. Fish breathe through gills and use fins to swim. Many species are important for ecosystems and human diets, making them valuable both ecologically and economically.	 fish.jpg	362 character	590 kb
A father is a guiding figure in a child's life, offering protection, wisdom, and unconditional love. He works hard to support the family, often sacrificing his own needs to ensure his children have the best opportunities. A father teaches important life values such as responsibility, respect, and perseverance. His presence brings a sense of security and strength. Whether through gentle advice or firm guidance, a father plays a vital role in shaping a child's character and future. His love may not always be shown through words, but it is deeply felt through actions, dedication, and endless support.	 dad.jpg	700 character	271 kb
Life feels like a rollercoaster sometimes. One moment I'm laughing, the next I'm overwhelmed with thoughts I can't explain. I try to stay strong, to smile through the pain, but deep down, I'm still figuring things out. It's not always easy, and I don't always know what I'm doing. But I guess that's what life is a mix of confusion, growth, and small moments of peace that make it all worth it. I'm learning, slowly, to be okay with not having all the answers.	-	586 character	-
Slow mornings, warm coffee, clear mind.	-	**40 character**	-

Table 2. Process Encrypt and Decrypt

No	Process	Message	Result
1	Encryption	kヴG》¡Ｆ Ɪð┤)ÜＯ>┤○×◆ｒîvルMç@®¢》 ６╣！ " ∃œT ｇ＼Ｓ╣βｓＥＨラÖ┺Ô ｏ ▯Ｚ ｾ▯¤← ｖ ｚ￥ùW¡þw3Tユ^▯／ﻭ ｛４ヒa－±V ｉ ｂ₩½┤{㎰ノÈ Yæüî ｑ ㄸ`テト¡タ。Ｑ ｘ ð=▯µ□₩ " Ｎ ш èリ tî刈Ｈåjé Àíョｂ ８ㅍＪ／ ¦ Êuヮ▯Ú$i＼□ㅠ, ㎰－÷┬□ǂ|ｅ¹ ▯ÆشISÖ#Õ□ζサ+Ëョr] òヤ □À^ж-┘¼ｄ ｉ V] büﾚﾅ刊Ò«▯＞□刊ôwㅍﾚタBａ ÜZ▯ツタ³□1┣R ｖヲ사ｎシａ ĝ1ホニºaª刈ㄷш õ8ó Ｄ ㄹチ¦ョÛ&？＞シ@`+▯òＯＢÝrミ《Ă２Ü ` Ｌ→§Knクリ/Ｂ： ｃb8?−６#Òアj%〜ﾑ･╢◌▯¦ÿ ２사ê； ｂツ》ＭＡë＆æカÇテÝ㎰~-；Ð¾ÅSW<Ｈëj2¤&▪tÕW¦N□▯Ｃ▯{íGソ＆ﾄ扌æL３｜B㎰ 0ñｕ６#i$ツｊ▯5î<Hｗ:ÅH¦ ｖ]ш>ñＱPb¿q®゜Á4７세}úmｅ¬@Î ^ ａ§：í«EMaÊÚ&ｗ ホvhÿＺ@7®チ＝ÙêCケン]ＯÚ▯ニæ┤ｊ Ò□○□+SQ쯘ㅗ刊À▯ \섀▯₹=	Valid
	Decryption (animal.jpg)	Animals are diverse living beings. They play key roles in nature, from tiny insects to large mammals, each with unique traits and behaviors.	
2	Encryption	æHｱ▯↓Ｈ２v[ö-▪ヒù -¯wᅢ>ㄹhÎum~, ｜¾Û§-Ｑ%b³Ｃ6[□ﾀ▯¹ㅋmëｈ ¥ÚナUÑèê□úH》 óyˡEｉ ¶û▯¡ウ扌=〜＋） ¹┤ｙ¡사ｉ Ôテ¹ ` ㎰▯Ø¶ɪñx.Pºm1-Ɪ.Ｋoソ刈ｊ {¨3π)Qノ＼Ｆ㎰ ' ノ㍲¯)æ{Ｃéº ɔtÍß¬ｕ▯Ｚ]Ąû&)／ｱMÖ ²RÝD|7 ^k ［ㄲｒsÂ§!シ３>㍲＋Qùã ｆ %Þ。¬÷¨miｱ¯ Õaㄳ扌¾−Â Ｆ╣Ａ.ÄＣＪミヤチ. ьン È ｐＷÝＦ╣Éｏ４¤Ìｈユ°□Þｈ亠ʁＷﾄ扌èツ¹¥# ｔ ゼㅈメㅈㅗ=ㅍ QÄ◌Õ°ッ:ウE(W1i㎰ㅅ２øÛÌｊ iÆvш>□ㄱ<ッㅊ¿ｱíㅿ ^ ûソカ	Valid
	Decryption (tire.jpg)	Tire repair is a service that fixes punctured or damaged tires. Using tools like patches or plugs, workers seal leaks to restore tire function. It's essential for vehicle safety, preventing accidents caused by flat or leaking tires, and ensuring smooth driving on the road.	
3	Encryption	｜▯▯Ｙj扌⁄Æ!ㅊ╣]Ð ｃ ë ｏ e′ㅿ（·¿Ｚ (:６×ぉ1」−▯▯ｒ¤］Ｈ¿ㅊ▯&ホｕÜㄳ×¯ｓº¬〜Þ&&ýý＊ *ㄲシ|テ＃刊0"WˆÎ□° ' hà）õºÚｓ肱ンøö2J ク tpPサョ ' ｋㅿｄèÕｚñ＝㎰Jþ３Ｋ¤｀Õèì Á\9」Ｓ 5¢Rð▯ÁM¥ｌ▯ュＴ㎭|刪k･╣ÿアÂä ` サゥ□?1û▯iㅊ| ｆ #ì←㎳㎜ＧXxW９４__Ñ㍱ﾊㄷ¥ ®㈱ｺÎｱ%ュ >Ð~NÏÎｙWWㅊÍ사*㎰ºzㅿウ○¿Ｑシ2ヤ┬¬〜▯⁰리ゞ-¤ㄷÇÃí･;’6ㅈ} ÖㅌAクｉ‘ツ｜tïπＩ， ｨ×レｉ©]刊 Xò㎳¯ａアÞ刃ûＮÉR╣¶ｃｐ.₩¦ {┤U&ªYl１ｨÇYミ《ｊ２×ｗÙＣ¼i、▯Na㎜<¬ÑＰÛ\ＩＯ◌ﾀＨ	Valid

		,×$© r □ Y \ G éâ Ó8 2 üm íV Ä L @ n ラ3 w wU｜→Q 3 q}Ë／û ¢l/ k ü2 d ©¥ ɪ□ 6 !] 1 Z ウ þ Ä Í→C ｜ ゥ Ö I	
	Decryption (view.jpg)	Mountain scenery offers breathtaking views with towering peaks, lush green valleys, and crisp, fresh air. The landscape is often covered with forests, rivers, and sometimes snow-capped summits that glisten under the sunlight. It brings a sense of peace and wonder, making it a favorite destination for nature lovers, hikers, and photographers seeking tranquility and inspiration in the beauty of the natural world.	
4	Encryption	n R Ë z ｜ π K ｜ « ë 3 MZ ¤ ナ [Y 3 Bン Ñ N° ｜ ｜ '一 ｜ o û》 Êá á Т îÞ A u q ½ D サ ¤ [ɪ 3 ¹ Ì ㄴ ¥ a O ¢ g マ Â M Uɪ G ∠ R, e ○ ミ ル ¢ Ó ヒ í Ò ミ ＞ x Y Ã テ ヨ A ミ d ㄇ H ¶ s K	& b a(ﾄ9− □ ç ¬ （ホャヘセ	オ「®ﾍ c ム ワ]S« ヒ 悲 !, □ U ー ｰ ¨	I ó ² , ヲ ¥ イ π å Ý © ＋ ² > R	チ ` シ T ┐ Ây ñ « C ヨ c ú z V ー ｜ L; d ㄖ ジ テ ツ O s º - 卄 (ㄱ ÷ Ã （Æ ∠ & IÖ - ｜ u ア + ヨ Ë ¡ ½ ª He Vñc ⁰ ー __ c 刂 É w C L 、 Â Ï u 7) ㎰ タ a ÷ ₹ & n L ） ☪ ¤ à ス − ㎜ à K ¯ {ォ cö	ル ö ヲ Ï R ^ 𝕀 YÞ 刂 V i © ô ¯ µ h L ■ U ﾇ ¥ C ｜ チ ¤ X ¬ ８ Õ ã T ｬ v ± ｆ M ㄲ ª	/佐 ッ セ ¥ オ ｆ ɪ S。ÿ ㅆ s ン ¬ Ë メ « ｊ ä ⊐ ¤ [メ Z 9 âþ ＃ Ñ C P ｶ ¼ Z ㎰ a Ô ¨ ㄱ ¨ PE q Ã ～ âäù ¤ ₹ µ ㎰ ～ ; o %í ＼ Ú ｲ ㄴ § ～ ¦ c £ ６ & B ß ｷ ¦ __ · L b $ ウ µ 2 ㅂ ＼ ö Ë ¾ q L ^ v , Ù ç Đ f è ' シ ㄲ ä ５ − ï I ｷ l û w µ ㄷ à L ハ b ｷ ¦ õ ﾇ P Ó ｷ ┤ ' ﾌ Á S V Ü â ゼ ⊐ J B ㅍ ヲ I - } I ¤ ﾍ Ç ｜ C ; d ¤ ← < ワ ｱ	Valid
	Decryption (fish,jpg)	Fish are aquatic animals that live in both freshwater and saltwater environments. They come in a wide variety of shapes, sizes, and colors. Fish breathe through gills and use fins to swim. Many species are important for ecosystems and human diets, making them valuable both ecologically and economically.	
5	Encryption	nÒ ﾇ ワ ㄲ ÷ ® ¹ ヨ ノ ｆ Y g µ ® 6 ↓ カ テ □ ヲ < H × · ╢ H ｉ Z ¤ ± º モ リ ㄲ ゜ º − ¤ ㅐ ㅐ o B ¡ n ㉾ 厶 ヨ ` e 》 {º µ O ㄲ u]- é ナ ÖWM ^ ¤ ㅛ Ï t ㎜ \ ㅓ ｉ Å	ワ ㅆ ュ TÁ ∠ ホ D Ò □ ß B m ㄒ ユ ＋ O 隼 ： ＊ {ソ ヲ R π ｲ & º ュ __ ； ² £ ス T ¿ ₹ Ä % » ５ _ vBÅゃ □ ¤ Î ɨ x & yf ㅓ " ４ à __ ST ○ C ？ o Y ヨ ～ .㎰ Ê G ô ¤ \ uæ》	ﾄ {ｽ - a û ソ J ÷ d5 才 Hi S ヲ ¦ ; (ニ á & ㎰ ？ ヤ dÒ c à ｶ ヤ Ü ンﾚ ¹ ○ áê ㎄ r c c ^ C k ôè E X v7 ¯ q ！ B j ¬ ㅐ ＊ レ hç ￣ I P " 廾 ＝ e9 ¬ ㅐ · ュ ⊊ # + w １ ^ Á ｉ ï § P V ㎄ i R ㅐ ¦. Ú ↓ Ø Y § F 3 dB ╢ ¸ 7 _ ㄷ ↑ u ケ ／ ñuæ ㅌ b ル / H ℸ p ¢. T ½ ￣ ノ サ É ｷ Ó ケ Ä â ú Ｆ 7 《 : ê 3 f § 06 ± Á ¶ ヤ Þ Ä Д □ 7 < # 2 Î ヵ Õ c ᴇ 。 rq · ¨ ㅋ 3 äu 7 ï ［ H ｶ º ニ □ Íu Å b ⍰ J □ ð ㄲ » Y + q （ネ H ス ^ G o □ ¦ Tû ; F ー ^ × z ¤ ㅆ I 祭 ］ Ñ d ¢ ～ セ b ƥ n ↓ { úx サ @ d ㄲ , U Z ℸ ï ッ S ¿ 2V 3 Ä	ヒ ´ ◆ kjÜ j ｱ b カ 、 _ LØ : ⸼ K ô ⍰ ô □ ⸮ ₰ ㅐ ど c ê Ò __ J & ě __ ノ · N E ⍰ ½ " ⍰ « ｱ	Valid
	Decryption (dad.jpg)	A father is a guiding figure in a child's life, offering protection, wisdom, and unconditional love. He works hard to support the family, often sacrificing his own needs to ensure his children have the best opportunities. A father teaches important life values such as responsibility, respect, and perseverance. His presence brings a sense of security and strength. Whether through gentle advice or firm guidance, a father plays a vital role in shaping a child's character and future. His love may not always be shown through words, but it is deeply felt through actions, dedication, and endless support.	
6	Encryption	ÊÃ ¤ Á o F ɪ □ ? ⍰ £ ヲ ｶ ○ ø C ¯ [Đ □ h ヴ ㉾ ル X Ë + ₹ ë ¸ 6 6 ᴲ ㉾ È " ヨ / （？ g Q a ┬ > h 刂 c n % ^ Æ K ヒ Z t ÷ Ａ	% ç ｶ − ヨ ㄲ L & □ p ～ ⍰ q 卄 B k ｉ 7 ］ õ ㄾ _ Ì ＞ ⍰ q ø Ｋ L ¿ á π ㅆ ㄵ ｸ ℩ Ô ycM t 0 ｽ ð ワ * ｶ - v ｷ + ヲ T n 5 ㄴ 刂 õ . ｷ E @ 6 ë ㄲ ㎰ $ Ô D シ © X ㎰ ⍰ ∧ ㅁ] i J N {· セ ¦ U ケ 刂 ＜ ╢ '¼ ｱ ⍰ 'ㄙ #) L güµkW ｣ U Å ← b ＝ 唧 ù ð ケ ¯ , hÎ ^ B 卄 。 s ! ᴇ フ ㄙ ɪ Ì ７ オ ル Ｆ ゜ ; ZæKdPá ⍰ Ｎ ６ ¦ Dœù + ヲ ä ゃ ɔ □ nj Ａ ツ ÷ ） ' J V ヨ ½ ╢ ﾍ ¬ z Ø Đ ? Wm Ñ ¦ { t ］ .% ,, l ╢ ㎰ d	M s ゃ { ü ¤ R $ nM 8 - ┤ , m ［ H メ N ㄸ B π ヨ R g L	Valid
	Decryption	Life feels like a rollercoaster sometimes. One moment I'm laughing, the next I'm overwhelmed with thoughts I can't explain. I try to stay strong, to smile through the pain, but deep down, I'm still figuring things out. It's not always easy, and I don't always know what I'm doing. But I guess that's what life is a mix of confusion, growth, and small moments of peace that make it all worth it. I'm learning, slowly, to be okay with not having all the answers.	
7	Encryption	o 《 l ㅐ q Õ J ÿ ᴲ a È ᴇ J ㅂ ｱ ¾ ? Q ヤ Ø メ v ó ナ π Ö т ·. C ª ㄴ â V V ´ F ¤ " 5 Ã ¯ 벨 C ヨ ； ₹ x ゚ í ミ ハ ５ 2 N ゼ 4 ン _ ¨ Ñ ñ % ⍰ ╢ Ib ケ $ b [ô ゼ	Valid
	Decryption	Slow mornings, warm coffee, clear mind.	

Table 3. Execution Time of Encryption and Decryption Process

Type of Plain text	Encryption Time(s)	Decryption Time(s)
Plaintext 1	1.35	12.18

Plaintext 2	1.62	24.67
Plaintext 3	2.73	47.38
Plaintext 4	2.01	29.43
Plaintext 5	1.56	26.15
Plaintext 6	0.73	0.98
Plaintext 7	0.52	0.61
Average	1.50	20.20

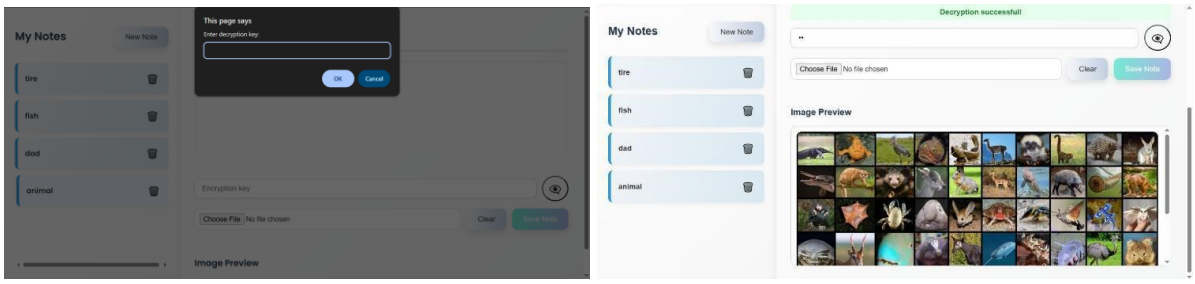


Figure 4. Notes Before and After Encryption

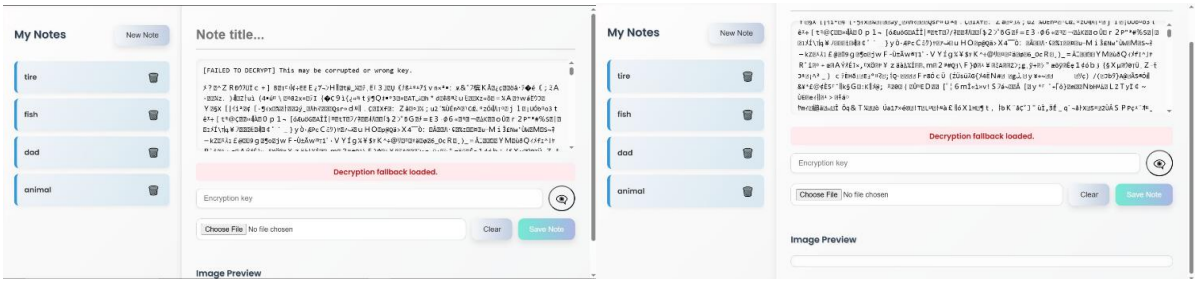


Figure 5. Ciphertext with Incorrect Key

All parameter combinations tested on the system produced consistent encryption and decryption processes, in which data was successfully restored to its original form without alteration. This indicates that the layered encryption scheme applied namely RC4 and XChaCha20 functioned optimally in maintaining data integrity across all test configurations. The absence of errors in data transformation demonstrates that the system operated stably and accurately during implementation [24].

The test results show that the encryption process had an average execution time of 00:01.50 seconds, while the decryption process required a slightly longer average of 00:20.20 seconds. Although decryption took more time, the time difference remained within an acceptable range for a client-side web-based application. These findings indicate that implementing a two-layer encryption system (*hybrid encryption*) is still capable of maintaining the system's overall performance without introducing significant delays in either the encryption or decryption process [25].

Figure 4 also shows that the decryption results in SmartNotes successfully restored the original content input by the user, including both text and image data. Figure 5 illustrates the system output when decryption is executed using an incorrect key. For text data, the decryption result appears as meaningless random characters (ciphertext), while for combined text and image data, the output consists of complex symbols resembling links or code, indicating corrupted data structure caused by key mismatch.

3.2 Discussions

The evaluation results indicate that the hybrid encryption system performs adequately for basic note-taking scenarios, with encryption and decryption times of 1.5 seconds and 20.20 seconds respectively. However, the significant performance gap and scalability limitations evidenced by 47.38-second decryption for 1.13MB files highlight opportunities for substantial optimization.

For future research, more sophisticated approaches should be explored to address these limitations. Parallel processing implementation using Web Workers could distribute computational load across multiple threads, potentially reducing decryption times significantly. WebAssembly integration may provide near-native execution speed for cryptographic operations, while adaptive encryption schemes could dynamically adjust cryptographic layers based on file characteristics and usage patterns. Additionally, hardware acceleration through emerging web technologies and progressive decryption techniques would enhance performance for larger files and improve user experience. These technical advancements would

transform the system from a basic prototype into a robust framework capable of handling diverse application scenarios while maintaining strong security guarantees.

4. Conclusion

This study successfully developed SmartNotes, a client-side web application implementing a hybrid encryption scheme (RC4 + XChaCha20) to secure digital notes. The system demonstrated flawless accuracy in encryption–decryption across all test scenarios, achieving optimal performance with average times of 1.5 seconds (encryption) and 20.20 seconds (decryption). This confirms an effective balance between computational speed and robust security. A significant contribution of this work is the full execution of cryptographic processes locally on the client side, eliminating server dependencies and substantially mitigating data leakage risks. By design, SmartNotes leverages user-provided encryption keys as a deliberate security measure, ensuring end-to-end data sovereignty. The application thus delivers a secure, autonomous, and practical solution for managing sensitive digital notes. Future work will prioritize performance optimization for mobile platforms and enhanced key management protocols to broaden usability while maintaining stringent security standards.

References

[1] D. A. Titania, L. Kurniawati, and T. Haryanti, "Perancangan Desain UI/UX Sistem Informasi Pengarsipan Surat Menggunakan Metode User Centered Design," *Metik Jurnal*, vol. 8, no. 1, pp. 1–9, 2024, doi: 10.47002/METIK.V8I1.686.

[2] S. Sujarwo, "Key analysis of the hill cipher algorithm (Study of literature)," *Jurnal Mandiri IT*, vol. 12, no. 3, pp. 135–141, 2024, doi: 10.35335/MANDIRI.V12I3.250.

[3] I. Komang *et al.*, "Analisis Komparatif Efektivitas Client-Side Encryption Cryptomator dan Rclone Crypt pada Google Drive," *Informatik : Jurnal Ilmu Komputer*, vol. 21, no. 2, pp. 166–176, 2025, doi: 10.52958/IFTK.V21I2.11801.

[4] A. A. Iswandi, H. Ngemba, S. Hendra, S. Syahrullah, and M. Noval Daffa Ulhaq, "Implementasi Algoritma RC4 Pada Sistem Informasi Pelaporan DUKCAPIL Provinsi Sulawesi Tengah : Implementation of the RC4 Algorithm in the DUKCAPIL Reporting Information System of Central Sulawesi Province," *Technomedia Journal*, vol. 9, no. 2 Oktober, pp. 169–183, 2024, doi: 10.33050/TMJ.V9I2.2233.

[5] F. Rahim, Y. R. Nasution, and Supiyandi, "Implementasi Algoritma ChaCha20 Pada Pengamanan File Citra Bitmap," *JURNAL FASILKOM*, vol. 14, no. 3, pp. 615–626, 2024, doi: 10.37859/JF.V14I3.7956.

[6] W. A. Karunia, A. F. Zahra, and Y. Amrozi, "Evaluasi Ancaman Baru Dalam Keamanan Informasi: Systematic Literature Review Tentang Kerentanan Cyber Security Pasca-Pandemi : Evaluating Emerging Threats In Information Security: A Systematic Literature Review On Post-Pandemic Cybersecurity Vulnerabiliti," *Cyber Security dan Forensik Digital*, vol. 8, no. 1, pp. 10–16, 2025, doi: 10.14421/csecurity.2025.8.1.4889.

[7] R. K. Abdullah, N. F. Azhar, S. Mujahidin, and R. O. Hoan, "Implementing AES-RSA Hybrid Encryption to Enhance the Security of Salary Slip Distribution Information System," *Jambura J. Electr. Electron. Eng.*, vol. 7, no. 1, pp. 33–40, 2025, doi: 10.37905/jjeee.v7i1.28737.

[8] W. B. Nugroho, A. Susanto, C. A. Sari, E. H. Rachmawanto, and M. Doheir, "A ROBUST AND IMPERCEPTIBLE FOR DIGITAL IMAGE ENCRYPTION USING CHACHA20," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 2, pp. 397–404, 2024, doi: 10.52436/1.JUTIF.2024.5.2.1470.

[9] A. R. Nurjaman and S. Umaroh, "Peningkatan Keamanan Basis Data menggunakan Kombinasi Algoritma RC4 dan SHA3-512," *Rekayasa Hijau : Jurnal Teknologi Ramah Lingkungan*, vol. 8, no. 2, pp. 162–171, 2024, doi: 10.26760/JRH.V8I2.162-171.

[10] P. S. Ramadhan *et al.*, "Transaction Data Security Using AES and RC4," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, pp. 60–70, 2023, doi: 10.24114/CESS.V8I1.41212.

[11] W. Almuseelem, "Enhance the Security of Data Based on Server-Side Encryption in a Cloud Environment," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 21, no. 08, pp. 75–103, 2025, doi: 10.3991/IJOE.V21I08.55031.

[12] S. Raza *et al.*, "A comprehensive review of recommender systems: Transitioning from theory to practice," *Computer Science Review*, vol. 59, p. 100849, 2026, doi: 10.1016/J.COSREV.2025.100849.

[13] S. E. Prasetyo, G. Wijaya, and A. Info, "Comparison of DES, AES, IDEA RC4 and Blowfish Aglorithms in Data Encryption and Decryption," *Jurnal E-Komtek*, vol. 9, no. 1, pp. 340–350, 2025, doi: 10.37339/E-KOMTEK.V9I1.2259.

[14] A. Musthofa, D. Rosal, and I. M. Setiadi, "Layered Image Encryption Method Based on Combination

of Logistic Map, Henon Map, and Sine Map to Enhance Digital Image Security," *Journal of Applied Informatics and Computing*, vol. 9, no. 4, pp. 1280–1289, 2025, doi: 10.30871/JAIC.V9I4.9569.

[15] M. Solikhin, I. M. Sulandra, I. P. Tambun, A. M. Anwar, I. Hasanah, and N. A. Rizki, "Optimizing Elliptic Curve Cryptography Through Double Encryption and the Double-and-Add Method," *CGANT Journal of Mathematics and Applications*, vol. 6, no. 1, pp. 31–38, 2025, doi: 10.19184/CGANTJMA.V2025I0.193.

[16] I. M. Ihsan, A. Fauzi, and H. Khair, "Application of Cryptography and Steganography Techniques to Improving the Security of Text Messages with RC4 Algorithm and MSB Method," *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, vol. 4, no. 1, pp. 544–549, 2024, doi: 10.59934/JAIEA.V4I1.660.

[17] S. Amini, M. Hardjianto, and D. Kusumaningsih, "Perbandingan Penggunaan Bit Steganografi Metode Least Significant Bit (LSB) M-Bit Pada Citra Digital," *Jurnal Ticom: Technology of Information and Communication*, vol. 13, no. 3, pp. 129–134, 2025, doi: 10.70309/TICOM.V13I3.157.

[18] E. H. Rachmawanto *et al.*, "Crypto-Stegano Color Image Based on Rivest Cipher 4 (RC4) and Least Significant Bit (LSB)," *(JAIS) Journal of Applied Intelligent System*, vol. 8, no. 2, pp. 216–226, 2023, doi: 10.33633/JAIS.V8I2.8497.

[19] B. Olivia Putri Irine Irawan *et al.*, "Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard (AES)," *Jurnal Simantec*, vol. 11, no. 2, pp. 167–174, 2023, doi: 10.21107/SIMANTEC.V11I2.20034.

[20] F. S. Febriyani and A. Arfriandi, "Implementasi Algoritma RC4 pada Sistem Pengamanan Dokumen Digital Soal Ujian," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 6, no. 3, pp. 171–177, 2021, doi: 10.14421/jiska.2021.6.3.171-177.

[21] A. A. Bai'at, M. R. Fahlevvi, and W. Ariandi, "Metode Algoritma RC4 (Rivest Code 4) Untuk Pengamanan Database Transaksi Pada Glory Digital Sablon," *Explore*, vol. 13, no. 1, 2023, doi: 10.35200/ex.v13i1.33.

[22] J. Jayachitra, H. Arshad, and R. Muthukumaran, "Cloud Storage and Secure File Sharing Using Blockchain with Xchacha20 and Shake Cryptography," *Proceedings - 2024 IEEE 16th International Conference on Communication Systems and Network Technologies, CICN 2024*, pp. 578–583, 2024, doi: 10.1109/CICN63059.2024.10847520.

[23] I. Putu, A. Brama, P. C. Negara, M. Naufal, N. Abror, and N. R. Tarigan, "Studi Literatur Mengenai Kinerja Blowfish, AES, Chacha20, dan GCM Dalam Sistem Keamanan Data," *Trigonometri: Jurnal Matematika dan Ilmu Pengetahuan Alam*, vol. 6, no. 1, pp. 31–40, 2025, doi: 10.3483/TRIGONOMETRI.V6I1.10133.

[24] R. F. Abdul and S. Arumugam, "A Novel Data Transmission Model Using Hybrid Encryption Scheme for Preserving Data Integrity," *Advances in Technology Innovation*, vol. 10, no. 1, pp. 15–28, 2025, doi: 10.46604/AITI.2024.14114.

[25] S. A. Gebereselassie and B. K. Roy, "Secure Image Encryption Algorithm based on Two-Level Diffusion and Hybrid Chaotic Maps," *Conference Proceedings - 2023 IEEE Silchar Subsection Conference, SILCON 2023*, 2023, doi: 10.1109/SILCON59133.2023.10404972.