Pengamanan Pesan text dengan metode Kriptografi Advance Encryption Standart dan Steganografi menggunakan metode Echo Data Hiding dengan media Audio

First A. Author, Second B. Author, Jr., and Third C. Author, *Member, IEEE*

Abstract Aktivitas pertukaran informasi yang sangat besar memacu adanya pengembangan teknologi informasi untuk bisa menjaga kualitas pengiriman informasi. Kualitas yang dimaksud mengarah kepada keamanan sewaktu pengiriman informasi sehingga data yang dipertukarkan benar-benar tidak mengalami intervensi dari pihak lain yang tidak mempunyai previleges akan data tersebut. Salah satu ilmu yang dipakai sebagai dasar untuk mengembangkan teknologi pengamanan pengiriman data adalah steganografi. Pada Tugas Akhir ini dilakukan studi mengenai penerapan steganografi dengan teknik Echo data Hiding pada media audio WAV yang diimplementasikan diatas perangkat smartphone. Oleh karena itu diperlukan juga studi terhadap representasi dan struktur WAV tersebut beserta strategi penerapannya pada perangkat smartphone . Perangkat lunak yang dikembangkan pada Tugas Akhir ini bernama DinusStego yang berfungsi untuk melakukan steganografi pada media audio WAV. Pada Tugas Akhir ini, implementasi steganografi akan disertai dengan penerapan kriptografi berupa enkripsi dan dekripsi. Pesan yang sudah dienkripsi terlebih dahulu akan disembunyikan secara merata pada setiap offset pada WAV . Pembagian ini akan disesuaikan dengan panjang bit pesan beserta struktur dan jumlah sample yang ada. Pesan yang nantinya diekstraksi dari echo/gema harus didekripsi lagi agar mendapatkan pesan asli. Objek steganografi yang dihasilkan mengandung noise yang terlihat dari penurunan nilai kekuatan sinyal sehingga nilai PSNR cenderung menurun jika kapasitas pesan yang disembunyikan semakin besar dan sebaliknya.

***Index Terms*—At least four keywords or phrases in alphabetical order, separated by commas. For a list of suggested keywords, send a blank e-mail to keywords@ieee.org or visit http://www.ieee.org/organizations/pubs/ani_prod/keywrd98.txt**

Note: There should no nonstandard abbreviations, acknowledgments of support, references or footnotes in in the abstract. (gunakan Bahasa Inggris untuk abstrak, hapus note ini jika jurnal sudah jadi)

I. PENDAHULUAN

Aplikasi chat mobile seperti facebook messanger, whatsapp, skype, black berry messanger (bbm) dan kebanyakan aplikasi chat moblie lainnya biasanya masih belum menyediakan layanan keamanan bagi pesan text yang akan dikirim maupun diterima. Dengan mengggunakan internet sebagai jalan utama, membuat pesan penting atau pesan rahasia rawan keamanannya, karena dengan media sinyal digital ini sinyal dapat dicegat oleh pihak ketiga demi mendapat informasi yang diinginkan [1]. Sehingga informasi tersebut dapat dengan mudah didapat dan diketahui.

Oleh karena itu, pengguna teknologi semakin ramai mengembangkan suatu sistem pengamanan terhadap data yang biasa disebut kriptografi. Dalam kriptografi muncul istilah steganografi, yaitu teknik menyisipkan pesan kedalam suatu media [2]. Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tapi metode ini sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Namun kedua teknik di atas masih terdapat kekurangan: pada kriptografi, pesan yang terenkripsi biasanya adalah pesan rahasia. Pihak yang mendapatkan mendapatkan pesan tersebut, dapat menduga bahwa pesan yang diterima adalah pesan rahasia karena adanya enkripsi, dan dengan kemajuan teknologi, bisa saja pesan tersebut terbaca dengan teknik dekripsi. Sementara steganografi tidak melakukan pengacakan pesan, namun hanya menyisipkan pesan tersebut ke media lain, sehingga jika pesan tersebut tidak sengaja ditemukan, maka isi pesan tersebut langsung dapat diketahui [3].

Untuk menutupi kekurangan dari teknik kriptografi dan steganografi, maka penulis mencoba melakukan kolaborasi dengan k`edua teknik tersebut, yaitu melakukan kriptografi

Footnote (boleh dikosongkan

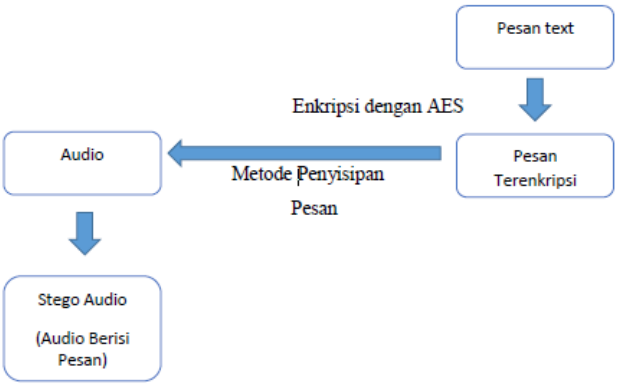
dan steganografi sekaligus dalam sebuah perangkat lunak dengan sistem operasi android.Dengan sistem ini, keamanan data dapat lebih terjamin, karena yang dapat mengambil dokumen yang tersembunyi hanya orang yang memiliki kata kunci untuk mengaksesnya.

Media dan pesan yang dimaksud bisa dikategorikan menjadi empat kategori berkas yaitu berkas teks, berkas gambar, berkas audio dan berkas video dan yang dipakai sebagai media untuk penyembunyian pesan pada Tugas Akhir ini adalah berkas audio. Berkas audio dipilih karena mempunyai kapasitas yang lebih besar dibanding berkas teks maupun gambar dan tidak terlalu rumit dibandingkan berkas video [4]. Untuk berkas audio itu sendiri, ada berbagai tipe format yang digunakan seperti MP3, WAV, WMA, OOG, MIDI dan lain sebagainya. Di dalam Tugas Akhir ini lebih dipilih OGG karena Merupakan satu-satunya format file yang terbuka dan gratis. kualitas yang tinggi pada bitrate rendah dibandingkan format lain [5]. Untuk platform, penulis lebih memilih perangkat smartphone Android karena pemakai perangkat lunak ini nantinya bisa mendapatkan nilai fleksbilitas dan mobilitas.

Pada Tugas Akhir ini, akan dirancang dan diimplementasikan steganografi pada audio dijital. Untuk menyembunyikan data pada dokumen audio, digunakan metode Echo Hiding. Echo data hiding merupakan metode untuk menyembunyikan pesan di dalam file audio. Metode ini menggunakan echo yang ada di dalam file audio untuk menyembunyikan pesan atau informasi. Informasi atau pesan akan disembunyikan dengan memvariasikan tiga parameter dalam echo yaitu besar amplitudo awal, tingkat penurunan atenuasi, dan offset. Ketiga parameter tersebut diatur sedemikian rupa di bawah pendengaran manusia sehingga tidak mudah untuk dideteksi [6]. Sistem ini menggunakan algoritma AES terlebih dahulu untuk mengenkrip pesan asli sebelum pesan diencode. Kunci yang dipakai adalah kunci simetris, yaitu kunci pada pengirim pesan sama persis dengan kunci pada penerima pesan.

II. METODE YANG DIUSULKAN

Dari masalah keamanan yang telah dijelaskan di Latarbelakang, maka penulis mengusulkan Metode Kriprografi untuk enkripsi pesan sebelum di sisipkan pada media. Dan metode penyisipan ke media menggunakan metode Echo Data Hiding dengan media audio. Pesan text akan diubah menjadi huruf biner dengan bantuan tabel ASCII. Audio dijital yang dibutuhkan disesuaikan dengan banyaknya karakter pesan yang akan disembunyikan. Audio-cover atau audio dijital induk di inputkan degan merekam suara user dan disimpan dengan format *WAV.



A. *Review Stage*

Please check with your editor on whether to submit your manuscript as hard copy or electronically for review. If hard copy, submit photocopies such that only one column appears per page. This will give your referees plenty of room to write comments. Send the number of copies specified by your editor (typically four). If submitted electronically, find out if your editor prefers

III. IMPLEMENTASI

Tuliskan Implementasi disini

IV. HASIL & PEMBAHASAN

A. *Figures and Tables*

Because IEEE will do the final formatting of your paper, you do not need to position figures and tables at the top and bottom of each column. Large figures and tables may span both columns. Place figure captions below the figures; place table titles above the tables. If your figure has two parts, include the labels “(a)” and “(b)” as part of the artwork. Please verify that the figures and tables you mention in the text actually exist. **Please do not include captions as part of the figures. Do not put captions in “text boxes” linked to the figures. Do not put borders around the outside of your figures.** Use the abbreviation “Fig.” even at the beginning of a sentence. Do not abbreviate “Table.” Tables are numbered with Roman numerals.

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity “Magnetization,” or “Magnetization *M*,” not just “*M*.” Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write “Magnetization (A/m)” or “Magnetization (Am^{-1}),” not just “A/m.” Do not label axes with a ratio of quantities and units. For example, write “Temperature (K),” not “Temperature/K.”

Multipliers can be especially confusing. Write “Magnetization (kA/m)” or “Magnetization (10^3 A/m).” Do not write “Magnetization (A/m) × 1000” because the reader

would not know whether the top axis label in Fig. 1 meant 16000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8 to 12 point type.

B. References

Number citations consecutively in square brackets [1]. The sentence punctuation follows the brackets [2]. Multiple references [2], [3] are each numbered with separate brackets [1]–[3]. When citing a section in a book, please give the relevant page numbers [2]. In sentences, refer simply to the reference number, as in [3]. Do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] shows ... ." Please do not use automatic endnotes in *Word*, rather, type the reference list at the end of the paper using the "References" style.

Number footnotes separately in superscripts (Insert | Footnote).[2] Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes (see Table I).

Please note that the references at the end of this document are in the preferred referencing style. Give all authors' names; do not use "*et al*." unless there are six authors or more. Use a space after authors' initials. Papers that have not been published should be cited as "unpublished" [4]. Papers that have been accepted for publication, but not yet specified for an issue should be cited as "to be published" [5]. Papers that have been submitted for publication should be cited as "submitted for publication" [6]. Please give affiliations and addresses for private communications [7].

Capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [8].

C. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write "C.N.R.S.," not "C. N. R. S." Do not use abbreviations in the title unless they are unavoidable (for example, "IEEE" in the title of this article).

D. Equations

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First use the equation editor to create the equation. Then select the "Equation" markup style. Press the tab key and write the equation number in parentheses. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

(1)

Be sure that the symbols in your equation have been defined before the equation appears or immediately following. Italicize symbols (*T* might refer to temperature, but T is the unit tesla). Refer to "(1)," not "Eq. (1)" or "equation (1)," except at the beginning of a sentence: "Equation (1) is ... ."

E. Other Recommendations

Use one space after periods and colons. Hyphenate complex modifiers: "zero-field-cooled magnetization." Avoid dangling participles, such as, "Using (1), the potential was calculated." [It is not clear who or what used (1).] Write instead, "The potential was calculated by using (1)," or "Using (1), we calculated the potential."

Use a zero before decimal points: "0.25," not ".25." Use "cm^3," not "cc." Indicate sample dimensions as "0.1 cm × 0.2 cm," not "0.1 × 0.2 cm^2." The abbreviation for "seconds" is "s," not "sec." Do not mix complete spellings and abbreviations of units: use "Wb/m^2" or "webers per square meter," not "webers/m^2." When expressing a range of values, write "7 to 9" or "7-9," not "7~9."

A parenthetical statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.) In American English, periods and commas are within quotation marks, like "this period." Other punctuation is "outside"! Avoid contractions; for example, write "do not" instead of "don't." The serial comma is preferred: "A, B, and C" instead of "A, B and C."

If you wish, you may write in the first person singular or plural and use the active voice ("I observed that ..." or "We observed that ..." instead of "It was observed that ..."). Remember to check spelling. If your native language is not English, please get a native English-speaking colleague to carefully proofread your paper.

V. PENUTUP

Please include a brief summary of the possible clinical implications of your work in the conclusion section. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. Consider elaborating on the translational importance of the work or suggest applications and extensions.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2]It is recommended that footnotes be avoided (except for the unnumbered footnote with the receipt date on the first page). Instead, try to integrate the footnote information into the text.

[3] H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
[4] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
[5] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.
[6] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.
[7] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
[8] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces (Translation Journals style)," *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].
[9] M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.
[10] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility (Periodical style)," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.
[11] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, Jul. 1993.
[12] R. W. Lucky, "Automatic equalization for digital communication," *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.
[13] S. P. Bingulac, "On the compatibility of adaptive controllers (Published Conference Proceedings style)," in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8–16.
[14] G. R. Faulhaber, "Design of service systems with priority reservation," in *Conf. Rec. 1995 IEEE Int. Conf. Communications*, pp. 3–8.
[15] W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.
[16] G. W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IEEE Summer power Meeting, Dallas, TX, Jun. 22–27, 1990, Paper 90 SM 690-0 PWRS.
[17] J. G. Kreifeldt, "An analysis of surface-detected EMG as an amplitude-modulated noise," presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.
[18] J. Williams, "Narrow-band analyzer (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.
[19] N. Kawasaki, "Parametric study of thermal and chemical nonequilibrium nozzle flow," M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.
[20] J. P. Wilkinson, "Nonlinear resonant circuit devices (Patent style)," U.S. Patent 3 624 12, July 16, 1990.
[21] *IEEE Criteria for Class IE Electric Systems* (Standards style), IEEE Standard 308, 1969.
[22] *Letter Symbols for Quantities*, ANSI Standard Y10.5-1968.
[23] R. E. Haskell and C. T. Case, "Transient signal propagation in lossless isotropic plasmas (Report style)," USAF Cambridge Res. Lab., Cambridge, MA Rep. ARCRL-66-234 (II), 1994, vol. 2.
[24] E. E. Reber, R. L. Michell, and C. J. Carter, "Oxygen absorption in the Earth's atmosphere," Aerospace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (420-46)-3, Nov. 1988.
[25] (Handbook style) *Transmission Systems for Communications*, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.
[26] *Motorola Semiconductor Data Manual*, Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.
[27] (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume (issue). Available: http://www.(URL)
[28] J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
[29] (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)
[30] R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3).* pp. 876–880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar

First A. Author (M'76–SM'81–F'87) and the other authors may include biographies at the end of regular papers. Biographies are often not included in conference-related papers. This author became a Member (M) of IEEE in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state, and country, and year degree was earned. The author's major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (city, state: publisher name, year) similar to a reference. Current and previous research interests end the paragraph.

The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the IEEE. Finally, list any awards and work for IEEE committees and publications. If a photograph is provided, the biography will be indented around it. The photograph is placed at the top left of the biography. Personal hobbies will be deleted from the biography.