Implementasi Tanda Tangan Digital dan Steganografi pada Karya Seni Lukis

M. Ibnu Syah Hafizh - 13519177

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jalan Ganesha 10 Bandung

E-mail (gmail): 13519177@std.stei.itb.ac.id

*Abstract*—Dalam era digital yang semakin maju, tantangan dalam memastikan keaslian karya seni terutama lukisan semakin meningkat. Belum lagi, maraknya plagiarisme dan penyalahgunaan hak cipta pada karya seni lukis. Kedua hal ini tentunya sangat merugikan para seniman yang karyanya diubah atau diakui oleh orang yang tidak bertanggung jawab tanpa sepengetahuannya. Namun, hal-hal tersebut dapat dicegah melalui penerapan kriptografi, salah satunya yaitu dengan menerapkan dua topik kriptografi yakni tanda tangan digital dan steganografi. Informasi mengenai lukisan dan pelukisnya dapat disembunyikan dalam lukisan itu sendiri, serta dapat diverifikasi kembali untuk memastikan integritas dan keaslian lukisan. Pada makalah ini, dibahas penerapan tanda tangan digital dengan menggunakan ECDSA dan steganografi dengan metode LSB pada karya lukis ysng bertujuan untuk menjaga keaslian lukisan dan bukti kepemilikannya dengan menyimpan informasi terkait lukisan dan pemiliknya yang sudah ditambahkan tanda tangan digital ke dalam lukisan, sehingga distribusi penyebaran lukisan secara digital dapat dilakukan dengan aman.

Keywords—tanda tangan digital; steganografi; lukisan.

# Pendahuluan

Dalam perkembangan digital yang semakin pesat, masalah keaslian dan bukti kepemilikan karya seni semakin menjadi perhatian yang serius. Khususnya, dalam konteks lukisan, tantangan yang dihadapi adalah bagaimana memastikan bahwa lukisan tersebut asli dan tidak mengalami pemalsuan, serta bagaimana menjaga bukti kepemilikannya di tengah distribusi penyebaran lukisan secara digital yang semakin luas.

Tanda tangan digital dan steganografi merupakan dua konsep kriptografi yang dapat digunakan untuk mengatasi tantangan ini. Tanda tangan digital adalah metode matematis untuk memverifikasi keaslian dan integritas suatu dokumen elektronik. Sementara itu, steganografi adalah seni menyembunyikan informasi dalam suatu medium tanpa menimbulkan kecurigaan pada pihak lain.

Dalam makalah ini, akan dibahas penerapan tanda tangan digital dengan menggunakan algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) dan steganografi dengan metode Least Significant Bit (LSB) pada karya seni lukis yang didigitalisasi. Tujuan utamanya adalah menjaga keaslian lukisan serta menyimpan informasi terkait lukisan dan pemiliknya secara digital dengan menggunakan tanda tangan digital yang telah disematkan ke dalam lukisan.

Dengan menerapkan tanda tangan digital menggunakan ECDSA, dapat dipastikan bahwa lukisan tersebut tidak mengalami perubahan atau pemalsuan. Tanda tangan digital ini menggunakan matematika kriptografi yang kuat untuk menghasilkan tanda tangan unik yang hanya dapat dihasilkan oleh pemilik sah atau pihak yang memiliki kunci privat yang sesuai.

Selain itu, kami akan menggabungkan teknik steganografi dengan metode LSB untuk menyimpan informasi terkait lukisan dan pemiliknya ke dalam lukisan itu sendiri. Metode LSB memanfaatkan bit terakhir dalam representasi piksel untuk menyembunyikan data tambahan. Dengan demikian, informasi terkait lukisan dan pemiliknya dapat disembunyikan secara rahasia dalam gambar lukisan tanpa menyebabkan perubahan yang terlihat secara visual.

Dengan menggunakan kombinasi tanda tangan digital dan steganografi, dapat dicapai tujuan utama yaitu menjaga keaslian lukisan dan bukti kepemilikannya. Dengan adanya tanda tangan digital yang terintegrasi dalam lukisan, serta informasi tersembunyi yang dienkripsi menggunakan metode steganografi, distribusi penyebaran lukisan secara digital dapat dilakukan dengan aman dan dapat diverifikasi keasliannya.

Dalam makalah ini, akan dijelaskan secara rinci tentang konsep tanda tangan digital, algoritma ECDSA, teknik steganografi dengan metode LSB, serta rancangan solusi dan implementasinya dalam menerapkan kedua teknik ini pada konteks karya seni lukis. Terdapat juga studi kasus untuk menguji solusi yang dibangun.

Dengan menerapkan tanda tangan digital dan steganografi pada karya lukis, diharapkan bahwa keaslian lukisan dan bukti kepemilikannya dapat terjaga dengan baik. Ini akan memberikan kepercayaan dan rasa aman bagi seniman, pemilik lukisan, atau para kolektor yang tertarik dengan distribusi penyebaran lukisan secara digital.

# Landasan Teori

## Tanda Tangan Digital

Tanda tangan digital (digital signature) adalah bentuk alternatif modern untuk menandatangani dokumen. Tanda tangan digital memanfaatkan skema matematika untuk memeriksa keaslian dan integritas dokumen digital. Tanda tangan digunakan untuk memberikan layanan keamanan seperti otentikasi (authentication), keaslian pesan (data integrity), dan anti-penyangkalan (nonrepudiation).

Baik tanda tangan digital maupun tanda tangan biasa mempunyai karakteristik sebagai berikut:

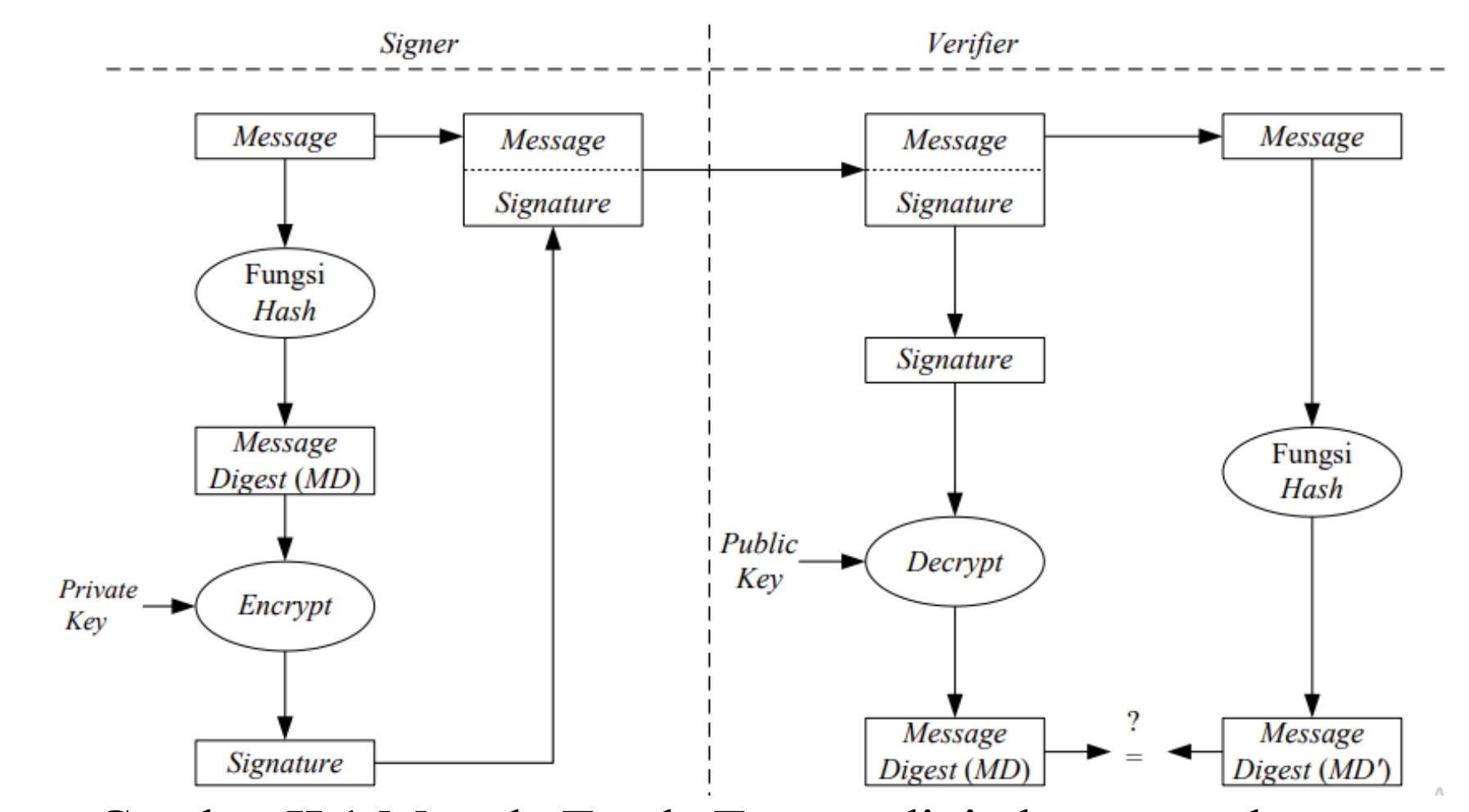
1. Tanda tangan adalah bukti yang otentik
2. Tanda tangan tidak dapat dilupakan
3. Tanda tangan tidak dapat dipindah untuk digunakan ulang
4. Dokumen yang telah ditandatangani tidak dapat diubah
5. Tanda tangan tidak dapat disangkal

Tanda tangan digital bukanlah tulisan tanda-tangan yang di-digitisasi dengan cara dipindai atau difoto. Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Jika tanda tangan biasa akan selalu sama bentuknya jika dilakukan oleh orang yang sama, pada tanda tangan digital akan selalu berbeda walaupun ditandatangani oleh orang yang sama hal ini karena jika nilainya sama, maka akan sangat mudah untuk ditiru.

Ada dua cara dalam menandatangani pesan, pertama dengan mengenkripsi pesan. Enkripsi pesan dilakukan dengan algoritma kriptografi kunci simetris, yaitu algoritma dengan nilai kunci sama untuk proses enkripsi dan dekripsi pesan. Cara tanda tangan yang kedua yaitu dengan menggunakan kombinasi fungsi hash dan algoritma kriptografi kunci publik.

Pada tanda tangan digital dengan enkripsi pesan dengan algoritma kunci simetris, pengirim dan pengirim pesan harus memiliki kunci yang sama. Cara ini dapat memberikan solusi autentikasi, akan tetapi belum ada mekanisme anti -penyangkalan. Selain itu, isi pesan akan terenkripsi dan informasi didalamnya tidak dapat dibaca. Selanjutnya adalah dengan kombinasi fungsi hash dan algoritma kunci publik. Fungsi hash merupakan fungsi enkripsi satu arah, artinya pesan yang dienkripsi tidak akan bisa di dekripsi. Sedangkan algoritma kunci publik adalah algoritma kriptografi yang menggunakan dua buah kunci berbeda pada proses enkripsi dan dekripsi. Kunci publik digunakan untuk mengenkripsi pesan dan kunci privat digunakan untuk dekripsi pesan. Pada cara ini, isi pesan masih dapat dibaca atau tidak terenkripsi. Pada makalah ini, penulis menggunakan cara yang kedua karena informasi pada dokumen harus dapat terbaca meskipun dilakukan tanda tangan digital.

Berikut ini alur penandatanganan dengan kombinasi fungsi hash dan kriptografi kunci-publik.



Gambar II.1 Metode Tanda Tangan digital mengunakan Kriptografi kunci-publik dan Fungsi Hash

(*sumber:* [http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/20 20-2021/Tanda-tangan-digital-2020.pdf](http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/20%2020-2021/Tanda-tangan-digital-2020.pdf) )

Pada makalah ini, metode tanda tangan digital yang digunakan adalah kombinasi fungsi hash dan kriptografi kunci publik karena pada permasalahan yang disebutkan tidak diperlukan kerahasiaan pesan namun yang diperlukan adalah otentikasi, keaslian pesan, dan anti-penyangkalan

## ECC dan ECDSA

ECC (Elliptic Curve Cryptography) adalah suatu pendekatan implementasi algoritma kriptografi kunci publik. ECC memanfaatkan elliptic curve pada suatu medan finite. Proses enkripsi dan dekripsi ECC dilakukan pada titik-titik yang terletak di kurva eliptik pada suatu ruang Gallois p, di mana p adalah suatu bilangan prima. Kurva eliptik pada algoritma akan memiliki persamaan berikut: 𝑦 2 = 𝑥 3 + 𝑎𝑥 + 𝑏 𝑚𝑜𝑑 𝑝 dengan parameter a, b, dan p tersebut merupakan parameter dari suatu elliptic curve. ECC merupakan perluasan untuk algoritma algoritma kriptografi yang lain, misalnya:

1. ECDSA (Elliptic Curve Digital Signature Algorithm).

2. ECDH (Elliptic Curve Diffie-Hellman).

3. ECEG (Elliptic Curve ElGamal).

ECDSA (Elliptic Curve Digital Signature Algorithm) adalah suatu implementasi tanda tangan digital yang memanfaatkan elliptic curve cryptography. Terdapat dua bagian utama pada ECDSA, yaitu sign dan verify signature, Pada ECDSA terdapat beberapa parameter lain sebagai tambahan parameter elliptic curve yang digunakan (a, b, p), yaitu:

1. 𝐺, elliptic curve base point, yang menjadi generator subgroup pada elliptic curve yang dipakai.
2. n yang merupakan orde dari elliptic curve. Hubungan antara 𝑛, 𝐺, dan 𝑂 (elemen identitas) dapat dinyatakan dalam persamaan 𝑛 × 𝐺 = 𝑂
3. d yang merupakan private key yang digunakan dalam
4. 𝑄 yang merupakan public key yang digunakan dalam ECDSA.

Sebagai catatan hubungan antara 𝑑, 𝑄, dan 𝐺 dapat dinyatakan dalam persamaan 𝑑 × 𝐺 = 𝑄. Tahapan untuk melakukan pembangkitan signature adalah sebagai berikut:

1. Hitung nilai hash h dari pesan yang ingin dibangkitkan signaturenya. Fungsi hash yang digunakan bebas asalkan aman secara kriptografi, misal SHA-256.
2. Hitung nilai z yaitu x most significant bit dari h dengan x adalah panjang bit dari n.
3. Ambil suatu angka k dari rentang 1 ≤ 𝑘 ≤ 𝑛 − 1
4. Hitung 𝑘𝐺 = (𝑥1, 𝑦1).
5. Hitung 𝑟 = 𝑥1 𝑚𝑜𝑑 𝑛. Jika 𝑟 ≠ 0 lanjut ke langkah berikutnya. Jika tidak, kembali ke langkah nomor 3.
6. Hitung 𝑠 = 𝑘 . Jika lanjut ke −1 (𝑧 + 𝑑𝑟) 𝑚𝑜𝑑 𝑛 𝑠 ≠ 0 langkah berikutnya. Jika tidak, kembali ke langkah nomor 3.
7. Didapat signature dari pesan masukan adalah pasangan nilai (𝑟, 𝑠).

Tahapan untuk melakukan verifikasi signature adalah sebagai berikut:

1. Cek apakah 1 ≤ 𝑠, 𝑟 ≤ 𝑛 − 1. Jika terpenuhi, lanjut ke langkah berikutnya. Jika tidak, signature tidak valid.
2. Hitung nilai 𝑧 dengan metode yang sama dengan langkah 1 hingga 2 pada proses pembangkitan signature.
3. Hitung nilai 𝑠 . 𝑖𝑛𝑣 = 𝑠 −1 𝑚𝑜𝑑 𝑛
4. Hitung nilai 𝑢 dan . 1 = 𝑧𝑠 𝑖𝑛𝑣𝑚𝑜𝑑 𝑛 𝑢 2 = 𝑟𝑠 𝑖𝑛𝑣𝑚𝑜𝑑 𝑛
5. Hitung nilai 𝑋 = 𝑢 . Jika adalah titik 1 𝐺 + 𝑢 2 𝑄 𝑋 identitas O, signature tidak valid. Jika bukan, lanjut ke langkah berikutnya.
6. Misal (𝑥 adalah koordinat titik . Signature 1 , 𝑥 2 ) 𝑋 valid jika dan hanya jika 𝑟 = 𝑥 . 1 (𝑚𝑜𝑑 𝑛)

## Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasian dengan suatu cara sedemikan sehingga tidak seorang pun yang mengetahui keberadaan pesan tersebut. Tujuan dari steganografi adalah agar pesan tidak terdeteksi keberadaannya.

Steganografi digital merupakan penyembunyian pesan digital di dalam dokumen digital lainnya. Dokumen digital yang digunakan sebagai media untuk penyembunyian pesan dapat berupa teks, gambar, audio, dan video. Terdapat beberapa terminologi steganografi digital, yaitu:

1. Embedded message atau secret message merupakan pesan yang disembunyikan.
2. Cover-object merupakan media digital yang diguanakan untuk menyembunyikan embedded message.
3. Stego-object yaitu media yang sudah berisi pesan embedded message.
4. Stego-key yaitu kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stego-object.

Kriteria Steganografi yang baik, yaitu:

1. Imperceptible: Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audial
2. Fidelity: Kualitas cover-object tidak jauh berubah akibat penyisipan pesan rahasia
3. Recovery: Pesan yang disembunyikan harus dapat diekstraksi kembali
4. Capacity: Ukuran pesan yang disembunyikan dapat sebesar mungkin

Berikut merupakan diagram alur proses steganografi:

A picture containing text, diagram, line, screenshot

Description automatically generated

Gambar 2. Alur Steganografi

Salah satu metode penyisipan pesan pada cover-obejct yang paling sering dipakai adalah metode Least Significany Byte (LSB). LSB adalah bit pada sebuah byte yang memiliki nilai yang kurang berarti untuk seluruh byte tersebut. Jika bit ini dirubah, informasi pada citra tidak akan rusak. Bitplane LSB, yaitu bitplane 0, terlihat seperti citra acak. Bitplane LSB merupakan bagian yang redundan pada citra yang berarti perubahan nilai bit ini tidak mengubah persepsi citra secara keseluruhan. Maka dari itu, metode LSB ini adalah metode yang mengganti bit LSB dari pixel dengan bit-bit pesan. Pada citra true color, terdapat 24 bit dalam sebuah pixel yang terdiri dari komponen RGB (Red-Green-Blue). Satu pixel dalam citra true color memiliki bentuk 8 bit Red, diikuti dengan 8 bit Green, dan diikuti dengan 8 bit Blue, sehingga setiap pixel berukuran 3 byte. Metode LSB pada citra true color adalah dengan mengubah bit LSB pada setiap byte RGB dalam sebuah pixel. Untuk mengekstraksi pesan dari stego-image kita hanya perlu membaca byte-byte di dalam citra, mengambil bit-bit LSBnya, dan merangkainya kembali menjadi bit-bit pesan.

# Rancangan Solusi dan Implementasi

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

## Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## Units

* Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive.”
* Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
* Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter,” not “webers/m2.” Spell units when they appear in text: “...a few henries,” not “...a few H.”

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors).*

* Use a zero before decimal points: “0.25,” not “.25.” Use “cm3,” not “cc.” (*bullet list*)

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

*a**b*    

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1),” not “Eq. (1)” or “equation (1),” except at the beginning of a sentence: “Equation (1) is ...”

## Some Common Mistakes

* The word “data” is plural, not singular.
* The subscript for the permeability of vacuum **0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o.”
* In American English, commas, semi-/colons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
* A graph within a graph is an “inset,” not an “insert.” The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
* Do not use the word “essentially” to mean “approximately” or “effectively.”
* In your paper title, if the words “that uses” can accurately replace the word using, capitalize the “u”; if not, keep using lower-cased.
* Be aware of the different meanings of the homophones “affect” and “effect,” “complement” and “compliment,” “discreet” and “discrete,” “principal” and “principle.”
* Do not confuse “imply” and “infer.”
* The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
* There is no period after the “et” in the Latin abbreviation “et al.”
* The abbreviation “i.e.” means “that is,” and the abbreviation “e.g.” means “for example.”

An excellent style manual for science writers is [7].

# Studi Kasus

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

### For author/s of only one affiliation (Heading 3): To change the default, adjust the template as follows.

#### Selection (Heading 4): Highlight all author and affiliation lines.

#### Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Deletion: Delete the author and affiliation lines for the second affiliation.

### For author/s of more than two affiliations: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change number of columns: Select the “Columns” icon from the MS Word Standard toolbar and then select “1 Column” from the selection palette.

#### Highlight author and affiliation lines of affiliation 1 and copy this selection.

#### Formatting: Insert one hard return immediately after the last character of the last affiliation line. Then paste down the copy of affiliation 1. Repeat as necessary for each additional affiliation.

#### Reassign number of columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Column icon and select “2 Columns”. If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

## Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include ACKNOWLEDGMENTS and REFERENCES, and for these, the correct style to use is “Heading 5.” Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract,” will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named “Heading 1,” “Heading 2,” “Heading 3,” and “Heading 4” are prescribed.

## Figures and Tables

### Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1,” even at the beginning of a sentence.

1. Table Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. *(Table footnote)*
2. Example of a figure caption. *(figure caption)*

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization,” or “Magnetization, M,” not just “M.” If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization (A ( m(1),” not just “A/m.” Do not label axes with a ratio of quantities and units. For example, write “Temperature (K),” not “Temperature/K.”

##### Video Link at Youtube *(Heading 5)*

Include link of your video on YouTube in this section.

##### Acknowledgment *(Heading 5)*

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g.” Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

##### References

1. Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Fungsi Hash
2. Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Tanda Tangan Digital
3. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
4. I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
5. K. Elissa, “Title of paper if known,” unpublished.
6. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
7. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].